ESCUELA DE JURISPRUDENCIA

TEMA:

INVESTIGACIÓN DE CIBERDELITOS COMO MEDIO DE TUTELA JUDICIAL EFECTIVA

Proyecto de investigación previo a la obtención de título de Abogada

Línea de investigación:

DERECHO, PARTICIPACION, GOBERNANZA, REGIMENES POLITICOS E INSTITUCIONALIDAD

Autora:

María Carolina Castillo Torres

Director:

Edgar Santiago Morales Morales Abg. Mg.

Ambato - Ecuador

Febrero 2024

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **MARIA CAROLINA CASTILLO TORRES,** con cédula de ciudadanía **1804277232**, autora del trabajo de graduación intitulado: "INVESTIGACIÓN DE CIBERDELITOS COMO MEDIO DE TUTELA JUDICIAL EFECTIVA", previa a la obtención del título profesional de **ABOGADA**, en la escuela de **JURISPRUDENCIA**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, febrero 2024

María Carolina Castillo Torres

CC. 1804277232

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DEL GRADO

Tema:

INVESTIGACIÓN DE CIBERDELITOS COMO MEDIO DE TUTELA JUDICIAL EFECTIVA

Líneas de Investigación:

DERECHO, PARTICIPACION, GOBERNANZA, REGIMENES POLITICOS E INSTITUCIONALIDAD.

Autora:

María Carolina Castillo Torres

Edgar Santiago Morales Morales, Ab. Mg. f. _____
1803294972
CALIFICADOR

Andrea Marlene Altamirano Zavala, Ab. Mg. f. _____
CALIFICADOR

Juan Carlos Manjarres Buenaño, Ab. Mg. f. _____
CALIFICADOR

Christian Danilo Gavilanes Domínguez, Ab. Mg. f. _____
DIRECTOR ESCUELA DE JURISPRUDENCIA

Diego Gonzalo Coca Chanalata, Dr. f. _____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Febrero de 2024

DEDICATORIA

A mi hermano, por forzarme a ser guía y ejemplo.

A mis padres, por confiar en mí.

A mis abuelos como símbolo de gratitud, y

A quien impulsó mi tema, y jamás me dejó rendirme en el proceso.

AGRADECIMIENTOS

Agradezco a mis padres, quienes me han dado la oportunidad de educarme y crecer continuamente en mis sueños, a mis abuelos que, con su cariño, amor y apoyo, me han dado la herencia de perseverancia y dedicación para poder culminar este proceso académico, a mi hermano quien con su admiración y preocupación me ha motivado a cumplir cada una de mis metas. Así, también doy gracias al Dr. Santiago Morales, mi tutor, docente y guía, quien depositó su confianza en mí, hasta cuando ni yo lo hacía, gracias por las múltiples correcciones, enseñanzas, y conversaciones existenciales que me encaminaban al objetivo cuando me sentía perdida. Una eterna gratitud a cada uno de los docentes quienes con su paciencia y dedicación impartieron sus conocimientos en este proceso educativo. Finalmente, gracias a todos mis compañeros, amigos, y conocidos que formaron parte de mi día a día durante esta maravillosa etapa.

RESUMEN

Esta investigación surge de la necesidad de proteger el derecho a la tutela judicial efectiva dentro de los casos de ciberdelitos, en razón que, en la actualidad, a las víctimas, se le dificulta el acceso a la justicia, tener una reparación integral y saber la verdad de los hechos en este ámbito, debido a que las investigaciones se encuentran en etapa de experimentación. Sumado aquello, se han evidenciado un incremento de delitos cometidos por estos medios, de los cuales no se llegan a concluir, de ahí la importancia del análisis.

La presente tiene como objetivo general analizar el proceso investigativo de ciberdelitos frente a la tutela judicial efectiva, para lo que se aplica una investigación de tipo cualitativa, en donde se analizan las cualidades del problema, mediante la aplicación de los métodos descriptivo y explicativo causal, para aterrizar en un estudio dogmático de la norma. Las unidades de análisis son la jurisprudencia, la ley y la doctrina. Como resultado se identifica el proceso de investigación de ciberdelitos en la legislación ecuatoriana, para garantizar la protección a la tutela judicial efectiva.

Palabras claves: Ciberdelitos, protección digital, tutela judicial efectiva.

ABSTRACT

This research arises from the need to protect the right to effective judicial protection in cases of cybercrime, because, at present, it is difficult for victims to have access to justice, to have a comprehensive reparation and to know the truth of the facts in this area, due to the fact that the investigations are in the experimental stage. In addition, there has been an increase in the number of crimes committed by these means, which are not concluded, hence the importance of the analysis.

The general objective of the present study is to analyze the investigative process of cybercrimes in the face of effective judicial protection, for which a qualitative type of research will be applied, where the qualities of the problem will be analyzed, through the application of descriptive and causal explanatory methods, to land in a dogmatic study of the norm. The units of analysis will be jurisprudence, law and doctrine. As a result, it is expected to identify the process of investigation of cybercrimes in Ecuadorian legislation, to ensure the protection of effective judicial protection.

Key Word: Cybercrime, digital protection, effective judicial protection.

INDICE GENERAL DE CONTENIDOS

INDICE DE TABLAS

INTRODUCCIÓN

El ordenamiento jurídico ecuatoriano tiene como objetivo principal proteger los derechos constitucionales y garantizar la armonía en la convivencia social. Con este propósito, se ha establecido un marco legal específico para cada ámbito, destinado a cumplir con dichos objetivos en sus respectivas competencias. En el ámbito del derecho penal, la regulación de conductas penalmente relevantes busca mantener la paz social, y el proceso penal se orienta hacia la búsqueda de la verdad y la garantía de reparación del bien jurídico de la víctima, sin descuidar los derechos de los sujetos procesales, en consonancia con el principio de tutela judicial efectiva.

La Constitución de la República del Ecuador de 2008, en su artículo 75, asegura la tutela judicial efectiva en los procesos, y el Código Orgánico Integral Penal de 2014 mantiene coherencia con esta norma suprema al garantizar dicho principio en la investigación penal.

Dentro de la investigación penal, se recopilan los elementos de convicción necesarios para formular cargos o archivar el proceso. La objetividad de la Fiscalía General del Estado, responsable de tutelar la acción penal pública en Ecuador, es crucial para determinar la responsabilidad de una persona imputada. Estos elementos de convicción, denominados pruebas durante la etapa procesal correspondiente, son esenciales en el proceso judicial penal, respaldando los argumentos de la fiscalía y la defensa para demostrar la culpabilidad o inocencia del acusado y contribuyendo a alcanzar la verdad.

En este trabajo investigativo, se emplea una metodología de investigación cualitativa que describe el problema de estudio y analiza el mismo objeto de estudio a través de la descripción de características, causas y efectos. Se utilizan métodos descriptivos y explicativos causales, así como métodos dogmáticos y exegéticos para analizar la normativa jurídica, la doctrina y la jurisprudencia que influyen en el ordenamiento jurídico ecuatoriano.

El objetivo general de la investigación es analizar el proceso investigativo de ciberdelitos en relación con la tutela judicial efectiva. Los objetivos específicos incluyen fundamentar doctrinaria y jurídicamente las variables de investigación, diagnosticar el acceso a la tutela judicial efectiva en el ordenamiento jurídico ecuatoriano e identificar el procedimiento de investigación de ciberdelitos en Ecuador según las fuentes del derecho utilizadas.

En el contexto ecuatoriano, los ciberdelitos, aunque contemplados en la normativa penal, no abarcan todas las conductas evidenciadas en la realidad. Por lo tanto, se considera fundamental reformar la normativa penal para incluir los delitos que aún no están tipificados, con el fin de garantizar la tutela judicial efectiva y lograr sentencias que reparen el bien jurídico de las víctimas. El análisis de la normativa y la situación actual del proceso de investigación de ciberdelitos respalda la necesidad e importancia de incluir conductas ausentes en la normativa actual, las cuales generan problemas y daños en los derechos de la sociedad.

En los últimos años, la tecnología a nivel mundial ha ido creciendo a un nivel inimaginable, es así que se han desarrollado los ciberdelitos, los mismos que según Saavedra (2023) en su investigación con el título “El ciberespacio escenario de confrontación”, analiza la forma en que el mundo existente en el internet puede provocar tantos beneficios como puede resultar ser tan perjudicial. El referido autor, emplea una investigación cualitativa dentro su trabajo, llegando a la conclusión que, así como existen algunos beneficios el internet también genera daños al patrimonio o a la integridad de una persona. Es por esta razón que, se relaciona con la presente investigación, toda vez que se analizan los ciberdelitos.

Asimismo, Ponce (2022) en su investigación titulada “DELITOS CIBERNETICOS” con enfoque cualitativo analiza la manera en cómo se dan los delitos a través del internet. En ese sentido menciona que, en Europa existe el Convenio sobre la Ciberdelincuencia, el mismo que fue promulgado en 2001, regulando de esta forma esta clase de delitos que afectan a toda la humanidad. La relación de esta investigación

realizada con la presente es que otorga las bases o el lineamiento esencial para poder entender los ciberdelitos.

En el mismo orden de ideas, López (2020) sostiene una investigación denominada “Los nuevos atractivos de internet”, en cuyo trabajo analiza todos los actos ilícitos que se pueden cometer sin que su crimen llegue a ser penalizado, esta investigación la realizó a través de un enfoque cualitativo, obteniendo como resultado que, debido al avance jurídico de algunos países alrededor del mundo en este tema, no se ha conseguido sancionar a los actores delictivos de los ciberdelitos. La unión de esta investigación con la presente, es que se analiza el vacío legal que aún existe en cuanto a los ciberdelitos.

Al respecto de las investigaciones en el plano internacional, Ferrer (2021) analiza en su investigación “La ciberdelincuencia en el mundo”, que, los ciberdelitos son un problema latente que, en la actualidad aún no han sido bien desarrollados por la normativa de algunos países. Esta investigación con enfoque cualitativo y con el uso del método analítico-sintético, tiene como conclusión que, dentro del orden jurídico mundial es necesario una regulación más directa y efectiva que se encargue de los delitos de internet que cada vez son más frecuentes y son más innovadores. Lo cual, sin duda la relaciona con la presente investigación, en tanto se busca analizar el mismo objeto de estudio.

En la misma línea de ideas, algunos ciberdelitos en Ecuador como: la revelación ilegal de información o el acceso no consentido a un sistema informático, los cuales, a pesar de estar contemplados en el Código Orgánico Integral Penal, no tienen una regulación efectiva, es decir no se acoplan al tipo penal descrito, pues existen muchas conductas que se quedan en el aire y sus víctimas no pueden ser resarcidas en sus bienes jurídicos que deben ser tutelados.

Para, Peña (2023) en su investigación: “Las nuevas reformas al COIP” determina que: “… los delitos con tinte cibernético necesitan más que tipificarlos en el código” (p. 15),

esta investigación con enfoque cualitativo, concluye que: el COIP (2014) es una norma completa, pero en la práctica se necesita desarrollar un manual o reglamento que direccione a los encargados de desarrollar el proceso penal a fin de tutelar los derechos de las víctimas de los ciberdelitos. Esta investigación guarda relación con la presente, en cuanto a la incorporación de los ciberdelitos en la normativa penal ecuatoriana.

En ese sentido, Parra (2022) sostiene dentro de su investigación “El ciber acoso” con enfoque cualitativo, busca analizar las conductas punibles que se llevan a cabo a través de la red, a fin de encontrar la vía más efectiva para sancionar a los delincuentes. Esta investigación concluye que el ciber acoso es una modalidad que ha existido desde el inicio de la red, en esta vía de comunicación e información existen peligros, igual o más peligrosos que en las calles y es por esta razón que guarda relación con la presente investigación, ya que lo que se busca es analizar todo el campo de los ciberdelitos, sus características y sus efectos jurídicos.

Por lo expuesto, resulta indispensable citar a Romo (2021) quien, dentro de su investigación “La ciberdelincuencia en Ecuador” estudia la característica de los ciberdelitos y la forma en que los ciber delincuentes actúan y logran pasar inidentificados por las autoridades estatales del Ecuador. Lo cual tiene relación directa con la presente investigación, porque el objeto de estudio es el mismo y el objetivo es analizar el proceso de investigación de esta clase de delitos en el ordenamiento jurídico ecuatoriano.

En tal sentido, la investigación “Los delincuentes de la red y su sanción penal”, realizada por Ponluisa (2021) con enfoque cualitativo, tuvo como objetivo general, analizar las consecuencias jurídicas de un ciberdelito en Ecuador, teniendo como resultados que, la norma penal ecuatoriana no contiene una regulación amplia y específica para los ciberdelitos, a pesar de su tipificación como conducta, aun el desarrollo es prematuro y hace falta una serie de regulaciones adicionales a fin de lograr un proceso penal sin vicios o deficiencias, lo cual se relaciona con la presente

investigación, toda vez que, como objetivo se tiene el analizar la normativa ecuatoriana en torno a este tema.

Con lo expuesto en líneas anteriores, se puede mencionar que el problema de investigación es que, la normativa penal ecuatoriana no contempla una regulación eficaz para investigar los ciberdelitos, por lo que, dentro del proceso penal como tal se vulneran derechos como la tutela judicial efectiva. La tutela judicial efectiva de acuerdo con Ávila (2016) es un derecho fundamental que garantiza a todas las personas el acceso a la justicia y la protección de sus derechos. En el contexto de los ciberdelitos, la falta de un eficaz proceso investigativo puede vulnerar este derecho, ya que los delincuentes pueden actuar de una manera impune y las víctimas llegan a quedar sin la debida protección.

Por lo tanto, es fundamental contar con un sistema judicial y de seguridad que esté preparado para enfrentar estos nuevos desafíos y garantizar la protección de los derechos de todos los ciudadanos. Entonces se podría decir que, si se regularía el proceso investigativo de ciberdelitos, se garantizaría el acceso a la tutela judicial efectiva.

La falta de una investigación adecuada puede significar la pérdida de pruebas importantes o la imposibilidad de identificar a los responsables, lo que dificulta la aplicación de la justicia y puede llevar a la impunidad de los delitos cometidos. Además, la falta de un proceso investigativo eficaz puede desincentivar la denuncia de los delitos, ya que los ciudadanos pueden sentir que no se tomarán medidas adecuadas para protegerlos y hacer justicia. En definitiva, la ausencia de un proceso investigativo eficaz de ciberdelitos vulnera el derecho a la tutela judicial efectiva, lo que a su vez puede generar una percepción de inseguridad en la sociedad y erosionar la confianza en el sistema judicial.

Dentro de la investigación, se plantea como hipótesis, la siguiente:
Si se regulase el proceso investigativo de ciberdelitos, se garantizaría el acceso a la tutela judicial efectiva.

La investigación se realiza bajo un enfoque cualitativo de investigación, toda vez que describe las variables de investigación de manera deductiva, por lo que, precisamente uno de los métodos a emplearse es el método deductivo, es decir se analiza el objeto de estudio desde premisas generales, hasta llegar a conclusiones particulares. Otro de los métodos de investigación empleados en la presente, es el método exegético, el cual de acuerdo con Salas (2020) consiste en analizar los parámetros normativos de un Estado a fin de verificar la forma en que se desarrolla el problema de investigación.

Otro de los métodos que se emplea por su naturaleza cualitativa, es el método analítico-sintético, por cuanto se analiza de forma detallada y minuciosa el objeto de estudio, sus variables, pero sobre todo su impacto en la población a investigar. Para la recolección de resultados se emplea la técnica de observación, gracias a la cual, se obtienen los datos de fuentes bibliográficas-documentales, asimismo se emplea la entrevista como una técnica destinada a obtener información desde la perspectiva de profesionales expertos en el tema.

En la actualidad, algunos ciberdelitos se encuentran tipificados en la norma penal del Ecuador, pero al ser un nuevo desafío para el derecho penal, hacen falta algunos lineamientos que permitan su correcto funcionamiento. La tutela judicial efectiva es un principio constitucional que dentro de la práctica del derecho se materializa incluso en un derecho y esta doble dimensión está protegida por el Estado ecuatoriano.

En función de este deber que tiene el Estado de garantizar la tutela judicial efectiva en todos los procesos, dentro de los ciberdelitos no debe haber excepción. En esta clase de delitos la investigación debe ser especializada y contar con un equipo de profesionales investigativos que tengan el conocimiento y la experiencia en esta rama, para que la investigación pueda concluir con elementos suficientes para continuar con el juicio. El mismo que, en su momento finalizará con una sentencia que contemple la

verdad, la justicia y en el caso de sancionar a una persona, lo haga garantizando la tutela judicial efectiva.

Investigar sobre ciberdelitos es de gran importancia por varias razones, entre las más significativas esta la protección de la seguridad, ya que los ciberdelitos pueden causar daños significativos a la seguridad de los individuos y organizaciones, como hurto de información confidencial, espionaje y sabotaje. Investigar y combatir estos delitos es fundamental para proteger la seguridad y privacidad de los usuarios, la integridad de las empresas y gobiernos, así como empezar con la prevención del delito; la investigación sobre ciberdelitos ayuda a identificar patrones y tendencias en la actividad criminal en línea, al comprender cómo se llevan a cabo los ciberataques, se pueden desarrollar medidas preventivas más efectivas para evitar futuros delitos, si se habla de justicia, los ciberdelitos pueden ser difíciles de detectar y probar, lo que puede dificultar la persecución de los delincuentes, investigar estos delitos es fundamental para recopilar pruebas y llevar a los responsables ante la justicia y la economía, los ciberdelitos pueden tener un impacto significativo en la economía, ya que pueden causar pérdidas financieras y dañar la reputación de las empresas.

Investigar y prevenir estos delitos es fundamental para proteger la economía global. Además de todo lo mencionado anteriormente, la importancia de la presente investigación es resolver la cantidad de ciberdelitos que en la actualidad se están quedando en la impunidad, se pretende investigar las razones de dicha afirmación, resolver las incógnitas del proceso investigativo de ciberdelitos, así como responder a la necesidad de proteger el derecho a la tutela judicial efectiva frente a los delitos cibernéticos.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Evolución dialéctica de las Investigaciones en los ciberdelitos

Los ciberdelitos como mecanismo delictivo en el mundo

Es necesario en primera instancia, definir a los ciberdelitos, por lo que, primero hay que entender a los mismos y su proceder. En ese sentido, Araujo (2017) determina que, la relación entre este tema y la tecnología es directa. Desde su inicio en la década de 1990, Internet cuenta con una vasta red electrónica. Esta red consta de millones de dispositivos que están íntimamente conectados entre sí. Con el avance de la tecnología en las últimas décadas en cada sector, el delito cibernético también aumenta día a día utilizando estas tecnologías.

Aproximadamente en el siglo XXI, los ciberdelitos, son conductas reprochables que involucran un medio tecnológico y una red de comunicación. La característica principal de este delito es que se comete a través de la red y es por esta razón que, su complejidad se convierte en la primera traba que poseen las autoridades estatales. Existen diferentes de delitos que vulneran diferentes bienes jurídicos tutelados, como el patrimonio, la integridad, el honor, etc. con el tiempo estos delitos han ido evolucionando, hasta el punto de que transacciones monetarias, dinero electrónico han sido creados con el fin de cometer actos ilícitos.

La tecnología a criterio de Aguirre (2020) es un espacio en la red que, brinda igualdad de oportunidades a todas las personas, es decir, permite acceder a todos los canales o portales existentes. Debido al incremento de internautas, la tecnología incrementa día a día y brinda el espacio necesario para la satisfacción de cualquier necesidad humana. En el mismo sentido en que la tecnología avanza, los delitos que se pueden producir a través de esta también lo hacen: y, es así que, se puede mencionar que el perfil de un ciber delincuente no tiene ninguna relación con la perspectiva de delito que se genera en un espacio físico. En palabras de Buenaventura (2021):

> “… quienes cometen delitos en el internet, son personas que están entre los 13 y 25 años de edad, que su nivel educativo y social es medio o alto, no son personas que en la vida real tengan o aparenten alguna falta en su conducta social. Toda vez que la característica de estos delitos es incluso en muchas ocasiones por distracción” (p. 25).

En tal sentido, es fundamental proteger a las personas de cualquier clase de ataque que se haga a través de sus plataformas cibernéticas. Por lo que, el uso de políticas o equipos que cuenten con las herramientas o programas especiales de protección ante accesos ilegales o no autorizados ese indispensable en la actualidad.

Según Días (2021) las facilidades de la tecnología informática no han salido sin inconvenientes. Aunque hace la vida tan rápida y rápido, pero arrojado bajo el eclipse de la amenaza del tipo de delincuencia más letal denominado "delito cibernético" sin computadoras, empresas enteras y operaciones gubernamentales casi dejarían de funcionar. La proliferación de computadoras baratas, poderosas y fáciles de usar ha permitido que más y más personas las usen y, más importante aún, confíe en ellos como parte de su forma de vida normal. Como empresas, agencias gubernamentales y las personas continúan confiando en ellos cada vez más, al igual que los delincuentes La restricción de los delitos cibernéticos es depende del análisis adecuado de su comportamiento y la comprensión de sus impactos en varios niveles de sociedad.

En el mismo orden de ideas, Roma (2022) sostiene que, el ciberespacio se encuentra repleto de actividades ilícitas, que van desde el uso no autorizado de imágenes hasta la facilitación de la difusión ilegal de contenido. En este contexto, se ha propuesto una teoría llamada la “Teoría del Comportamiento Planificado de Ajzen”, que, junto con el menos conocido modelo de la “Teoría del Flujo de Beveren”, ha sido examinada minuciosamente. Cuando se aplican en conjunto al ámbito de la piratería informática, estas teorías explican muchas de las características que se observan en la actividad de los primeros piratas informáticos.

Se muestra que la teoría del flujo proporciona una justificación para el desarrollo de piratas informáticos desde nuevos participantes hasta piratas informáticos expertos y, potencialmente, a delincuentes cibernéticos. A palabras de Roma (2022) el modelo Beveren de desarrollo de piratas informáticos se amplía para incorporar actores cibernéticos adicionales existentes en los campos de la guerra de la información y el delito cibernético. Se discuten las implicaciones de este modelo y, utilizando los resultados de la Teoría del Comportamiento Planificado, se identifican una serie de variables de control significativas. Se consideran las estrategias policiales para abordar el delito cibernético, y la piratería en particular, y se propone un enfoque integral para reducir de manera proactiva la propensión de los adolescentes a comenzar a piratear, como un paso inicial importante para abordar el problema más grave de la delincuencia informática.

Es este grupo social, quien más atraído se siente de la tecnología, al ser jóvenes y disponer de mucho más tiempo libre, los adolescentes son susceptibles, a cometer cualquier clase de acción en el internet incluso por distracción y pasatiempo. No son conscientes que, lo que al inicio puede tomárselo como un juego, con el devenir del tiempo se estaría convirtiendo en una serie de delitos que, lo conllevan a una responsabilidad penal. El mundo de internet hoy en día se ha convertido en una forma de vida paralela. El público ahora es capaz de hacer cosas que no eran imaginable hace unos años. Internet se está convirtiendo rápidamente en una forma de vida para millones de personas y también una forma de vida debido al crecimiento dependencia y confianza de la humanidad en estas máquinas.

Por su parte, el delito cibernético según Castañeda (2020) está emergiendo como una amenaza seria. Alrededor del mundo entero, diferentes gobiernos, departamentos de policía y unidades de inteligencia han comenzado a reaccionar. Las iniciativas para frenar las ciber amenazas transfronterizas están tomando forma. La policía india ha iniciado celdas cibernéticas especiales en todo el país y ha comenzó a capacitar al personal. Los titulares de las noticias contemporáneas parecen albergar regularmente tratamientos de una forma u otra de ciberdelincuencia, ya sea fraude, piratería

informática, piratería o material de abuso infantil en línea. En este documento, se desglosa el significado de ese término, se considera el impacto social y se analizan los posibles desarrollos futuros. Dada la influencia generalizada y profunda de Internet, es importante reconocer que, en términos de criminología, lo que sucede en línea puede tener un impacto en el mundo real y viceversa.

A medida que se automatizan más actividades comerciales y se utiliza un número cada vez mayor de computadoras para almacenar información confidencial, la necesidad de sistemas informáticos seguros se vuelve más evidente. Esta necesidad de acuerdo con Salas (2019) es aún más evidente cuando los sistemas y las aplicaciones se distribuyen y acceden a través de una red insegura, como Internet. Internet en sí se ha vuelto fundamental para los gobiernos, las empresas, las instituciones financieras y millones de usuarios cotidianos. Las redes de computadoras soportan una multitud de actividades cuya pérdida prácticamente paralizaría a estas organizaciones. Como consecuencia, los problemas de ciberseguridad se han convertido en problemas de seguridad nacional. Proteger Internet es una tarea difícil.

De acuerdo con Ponluisa (2021): “existe un modelo integral de investigaciones de delitos cibernéticos es importante para estandarizar la terminología, definición de requisitos y apoyo al desarrollo de nuevas técnicas y herramientas para los investigadores” (p. 42). Por lo que, se presenta un modelo de investigaciones que combina los modelos existentes, los generaliza y los extiende explícitamente para abordar determinadas actividades no incluidas en ellas. A diferencia de los modelos anteriores, este modelo representa explícitamente los flujos de información en una investigación y captura el alcance completo de una investigación, y no sólo el procesamiento de las pruebas y los resultados sino también se presenta la evaluación del modelo por parte de investigadores de delitos cibernéticos en ejercicio. Este nuevo modelo se compara con algunos modelos existentes importantes y se aplica a un modelo real de investigación.

La amenaza del ciberdelito continúa evolucionando y creciendo a medida que los delincuentes se adaptan a las nuevas medidas de seguridad y aprovechan los cambios en nuestro comportamiento en línea. Según Erazo (2019) la única constante parece ser nuestra vulnerabilidad: independientemente de los nuevos pasos que tomen empresas o individuos, los delincuentes siempre parecen estar un paso por delante. La amenaza del ciberdelito continúa evolucionando y creciendo, ya que los delincuentes se adaptan a las nuevas medidas de seguridad y aprovechan los cambios en nuestro comportamiento en línea. Para adelantarnos a los delincuentes, debemos cambiar la forma en que hacemos las cosas. Los líderes empresariales deben reconocer la amenaza y asegurarse de que su organización esté adecuadamente preparada y protegida.

En los últimos años, Internet ha cambiado muy rápidamente desde la educación, las empresas emergentes y los deportes hasta el medio de entretenimiento. Por lo tanto, Internet es el centro de conocimiento para todas y cada una de las personas que tienen poco conocimiento sobre cómo operar el navegador web o los dispositivos móviles. Para Ponluisa (2021): “El uso de Internet también contiene ventajas y desventajas” (p. 15). La peor desventaja de Internet es el cibercrimen, hoy en día, el delito cibernético es una amenaza emergente para todos los usuarios de Internet y computadoras, así como para la sociedad en general. Por lo tanto, el gobierno de varios países, los departamentos de policía y otros departamentos de inteligencia ahora están siendo estrictos y reaccionarios a estas amenazas cibernéticas emergentes y la propagación de los delitos cibernéticos.

Los gobiernos han comenzado a tomar iniciativas para eliminar los delitos cibernéticos de todo tipo junto con las amenazas cibernéticas transfronterizas, las operaciones de la web oscura, etc. Los gobiernos de todos los países, incluida la India, han comenzado a establecer celdas cibernéticas en todo el país y también las han vuelto funcionales mediante la educación del personal policial. en materia de prevención del ciberdelito.
La nueva tecnología está emergiendo rápidamente para combatir las crecientes amenazas de delitos cibernéticos, sin embargo, hay un componente importante de un

delito cibernético que la tecnología no siempre puede afectar y ese es el comportamiento humano. Para Bernal (2019) los seres humanos son vulnerables y fácilmente engañados, lo que hace que los avances tecnológicos por sí solos sean inadecuados en la lucha contra el delito cibernético. En su lugar, se debe adoptar un enfoque más holístico mediante el uso de la tecnología y una mejor comprensión de los factores humanos que hacen posible el delito cibernético.

Tipos y Características

Los ciberdelitos son conductas típicas, jurídicas y culpables que se encuentran, al igual que otros delitos, contenidos en una norma penal de diferentes Estados. En el caso específico del ordenamiento jurídico ecuatoriano, los ciberdelitos han sido llamados como delitos informáticos, los mismos que, actualmente en el Código Orgánico Integral Penal (2014) han incorporado dentro de sus últimas reformas. Así dentro de la citada norma, existen algunas conductas que sancionan a la utilización de plataformas electrónicas para cometer delitos como, por ejemplo:

> Artículo 103: Producción de pornografía con participación de menores. Aquella persona que capture, grabe, produzca, difunda, edite o modifique material visual, audiovisual, informático, electrónico, u otro tipo de soporte físico o formato, que incluya la representación real o simulada de desnudez o semidesnudas de menores en actitudes de naturaleza sexual, independientemente de la procedencia o el origen desconocido del material, será sancionada con una pena de privación de libertad que oscilará entre trece y dieciséis años (artículo 103).

Este tipo penal consiste principalmente en reproducir material sexual en donde se involucren a niños, niñas y adolescentes. La vía de proliferar este tipo de contenido generalmente es través del internet, por el avance mismo de la tecnología, la pornografía infantil es un fenómeno que se ha expandido a nivel mundial en segundos.

Otro de los delitos informáticos contemplados en el COIP (2014) es la violación a la intimidad, de la misma manera en que la pornografía se expandió a través del internet, es por medio de esta vía que, las personas pueden publicar o difundir contenido, fotos o datos de carácter estrictamente personal, en ese sentido la norma determina:

> Art. 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años (art. 178).

Es por ello que, la violación a la intimidad constituye un tipo penal de naturaleza informática, toda vez que, la esencia de este delito se consolida a través de la red.
Asimismo, el COIP (2014) prescribe un delito de carácter patrimonial:

> Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años (art. 190).

A través del tipo penal citado, se tiene que el ordenamiento jurídico ecuatoriano regula aquella conducta a través de la cual se irrumpe el funcionamiento de una red electrónica de una persona para beneficiarse a sí misma o a una tercera persona.
Otro de los delitos que contempla el COIP (2014) es la supresión, alteración o suposición de la identidad y estado civil, el cual se determina en el siguiente artículo:

> Art. 211.- Supresión, alteración o suposición de la identidad y estado civil.- La persona que ilegalmente impida, altere, añada o suprima la inscripción de los datos de identidad suyos o de otra persona en programas informáticos, partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la Dirección General de Registro Civil, Identificación y de Cedulación o sus dependencias o, inscriba como propia, en la Dirección General de Registro Civil, Identificación y Cedulación (Art. 211).

La persona que, a través de plataformas digitales, manipule o divulgue datos que se encuentren relacionados con la identidad de las personas, también está sancionado con una pena privativa de libertad. Esta es otra clase de los delitos informáticos en el Ecuador, el cual, en caso de verificarse su cometimiento, se deberá seguir el procedimiento estipulado para el efecto.

En ese sentido también se crea un delito conocido de acuerdo con el Código Orgánico Integral Penal (2014) como:

> Art. 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años (art. 229).

Es así que son diferentes los delitos que contempla la norma penal, de igual forma, se establece:

> Art. 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:
>
> 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma,

> contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.
>
> 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.
>
> 3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.
>
> 4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
>
> 5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (art. 230).

La norma legal ecuatoriana, también contempla en su artículo 231 el siguiente tipo penal:

> Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años (art. 321).

En el mismo sentido, los delitos informáticos en Ecuador se han delimitado en algunos tipos penales como, por ejemplo:

> Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años (art. 232).

Es por esta razón que, se puede mencionar que los delitos cibernéticos en Ecuador se encuentran regulados y la norma ya prevé las sanciones y consecuencias para cada caso. Tal es así que:

> Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.
>
> 1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años.
>
> 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

De igual forma, la falsificación informática es una conducta penal, que se contempla de la siguiente forma:

> Art. 234.1.- Falsificación informática:
>
> 1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.
>
> 2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena (art. 234.1).

Finalmente, la normativa penal, contempla un artículo exclusivo para definir algunos términos en cuanto a los delitos informáticos, esto con el fin, de que no existan confusiones en el plano de su aplicación.

> Art. 234.4.- Definiciones. - Para los efectos del presente Código, se considera:
>
> a. Contenido digital- El contenido digital es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico o canal de comunicación que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.
>
> b. Datos de tráfico. - Contenido digital relativo a una comunicación efectuada por medio de un sistema informático o canal de comunicación, generados por este sistema como elemento de una cadena de comunicación, indicando su origen, su destino, su trayecto, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente.
>
> c. Proveedor de servicios. - Cualquier entidad, pública o privada, nacional o internacional, que proporciona a los usuarios de sus servicios la

> capacidad de comunicarse a través de un sistema informático, o de cualquiera de las tecnologías de la información y comunicación, así como cualquier otra entidad que procese o almacene contenido digital en nombre y por cuenta de aquella entidad proveedora o de sus usuarios.
> d. Sistema informático. - Cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de contenido digital (art. 234.4).

Es por todo lo expuesto que, la normativa si cumple con su rol de regular las conductas conforme la evolución de la sociedad. Cada conducta debe ser analizada por el órgano legislativo de un Estado con el fin, de regular su conducta en sociedad y evitar que la convivencia social se vea involucrada.

Es igual de importante, mencionar que, dentro del artículo 173 del COIP (2014) se establece que aquellas personas que, a través de medios electrónicos, propongan encuentros con individuos menores de dieciocho años con la intención de llevar a cabo actos de naturaleza sexual o erótica, podrían enfrentar sanciones que incluyen penas privativas de libertad de hasta tres años (según lo establecido en el artículo 173 del COIP, 2014). Del mismo modo, se establece que aquellos que, haciendo uso de una identidad falsa o suplantando la identidad de otra persona mediante medios electrónicos o telemáticos, entablen comunicaciones de índole sexual o erótica con individuos menores de dieciocho años o con discapacidades, podrían ser condenados a penas privativas de libertad que oscilan entre tres y cinco años (de acuerdo con lo establecido en el artículo 176).

Cuando el acercamiento se logre mediante coacción o intimidación, o cuando se suplante la identidad de otra persona o se utilice un perfil falso para establecer comunicaciones de índole sexual o erótica, las sanciones varían entre tres y cinco años, como se establece en el artículo 174 del COIP. Además, de acuerdo con García (2022) dentro del mismo artículo, se encuentra una disposición que se refiere a la

oferta de servicios sexuales a menores de dieciocho años a través de medios electrónicos. Esta disposición indica que cualquier persona que utilice medios electrónicos o telemáticos, como correo electrónico, chat, mensajería instantánea, redes sociales, blogs, *fotoblogs*, juegos en línea o cualquier otro medio similar, para ofrecer servicios sexuales a menores de dieciocho años, podría ser condenada a penas privativas de libertad que oscilan entre siete y diez años.

Aquellos que, a través de medios electrónicos, ofrezcan servicios sexuales a menores de 18 años podrían enfrentar una pena privativa de libertad de 7 a 10 años, considerándose esto como un delito agravante. Los delitos definidos en los artículos 173 y 174 del COIP (2014) tienen como objetivo no solo prevenir la comisión de delitos informáticos, sino también abordar un problema aún más grave, que es la pornografía infantil, ya que se violan los derechos de los menores. Por lo tanto, es crucial que los países trabajen en conjunto a través de acuerdos de cooperación internacional para fortalecer la efectividad de estas leyes, dado que las redes de pornografía infantil operan simultáneamente desde diferentes naciones.

Además, hay que mencionar el artículo 178 de la norma penal ecuatoriana trata sobre la violación de la intimidad. Este artículo a palabras de Rodríguez (2018) establece que cualquier individuo que, sin contar con el consentimiento adecuado o la autorización legal, acceda de alguna manera a la divulgación de datos personales, grabaciones de voz, contenido de audio o video, así como otra información, podría ser condenado a una pena privativa de libertad que oscila entre uno y tres años. En otras palabras, también se considera un delito interferir en la privacidad de una persona y divulgar información confidencial, una práctica que lamentablemente se ha vuelto cada vez más común gracias a las redes sociales.

En relación al artículo 186 del COIP (2014) se hace referencia a la estafa, que se define como el acto en el cual una persona, con el propósito de obtener beneficios económicos para sí misma o para alguien más, utiliza la simulación de hechos falsos o la distorsión de hechos verdaderos, junto con la manipulación de otra persona para

inducirla al error, con el fin de perjudicar su propio patrimonio o el de un tercero. Este delito según Muñoz (2020) conlleva una pena de privación de libertad que varía entre cinco y siete años. En resumen, la estafa implica la manipulación de hechos con el objetivo de obtener beneficios para uno mismo o para otro a través de engaños previos que afectan a la víctima, y esto puede resultar en una pena de hasta siete años de prisión, especialmente cuando se trata de la alteración, clonación o modificación de dispositivos, como, por ejemplo, tarjetas de crédito o débito bancario.

Desde el artículo 191 hasta el 195 del COIP (2014) se abordan los delitos relacionados con el uso de dispositivos móviles. Esto se debe a que, en la actualidad, el uso de la tecnología móvil es ampliamente difundido en la sociedad. El artículo 191 de manera específica se enfoca en la reprogramación o alteración de la información de identificación de los dispositivos móviles. Según este artículo, cualquier persona que realice la reprogramación o modificación de la información de identificación de un dispositivo terminal móvil podría enfrentar una pena privativa de libertad que va de uno a tres años.

En cuanto a esta cuestión, la pena prevista es de uno a tres años en el contexto de la alteración de la información de identificación de dispositivos móviles que se encuentren registrados en la plataforma tecnológica de la Superintendencia de Telecomunicaciones. Esta medida forma parte de los esfuerzos para prevenir robos o actividades ilegales relacionadas con estos dispositivos.

En relación al artículo 192 del COIP (2014), se aborda el tema del intercambio, la venta y la compra de información de dispositivos móviles. Según este artículo, cualquier individuo que participe en el intercambio o la comercialización de bases de datos que contengan información de identificación de dispositivos terminales móviles podría enfrentar una pena de privación de libertad que oscila entre uno y tres años.

En el artículo 193 de la norma penal, también se aborda el tema del reemplazo de la identificación en los dispositivos móviles, lo que significa que aquellas personas que

sustituyan las etiquetas originales de fábrica en los terminales móviles que contienen información de identificación de estos equipos y las reemplacen con etiquetas que muestren información falsa o diferente a la original podrían enfrentar una pena de privación de libertad de uno a tres años.

En cuanto al artículo 194 del COIP (2014), se trata de la comercialización ilegal de terminales móviles, estableciendo que cualquier individuo que venda dispositivos móviles infringiendo las disposiciones y procedimientos establecidos en la normativa emitida por la autoridad competente de telecomunicaciones podría ser condenado a una pena de privación de libertad que va de uno a tres años.

Además, hay otros artículos relacionados con la divulgación de información, tanto en forma física como virtual, y las sanciones correspondientes. Por ejemplo, el artículo 195 del COIP (2014) se refiere a la infraestructura ilícita, que se define como aquella que posee elementos como equipos, bases de datos, programas y etiquetas que tienen la capacidad de reprogramar, modificar o alterar la información de identificación de un dispositivo móvil. Según este artículo, cualquier individuo que cuente con esta infraestructura podría enfrentar una pena de privación de libertad que oscila entre uno y tres años. De esta manera, se puede notar que la mayoría de las regulaciones relacionadas con delitos de información, que no involucran situaciones de naturaleza sexual, conllevan penas que van de uno a tres años de privación de la libertad.

Hasta la fecha, es relevante destacar que Ecuador aún no ha recibido una invitación formal para unirse al Convenio sobre la Ciberdelincuencia. No obstante, Rojas (2019) sostiene que, el país está evaluando la posibilidad de iniciar los trámites correspondientes para adherirse a este convenio. Esta consideración toma en cuenta la promulgación de su nuevo Código Orgánico Integral Penal, que aborda de manera exhaustiva la delincuencia informática.

Es relevante resaltar la importancia de difundir entre las comunidades las leyes que están diseñadas para salvaguardar a la sociedad de este tipo de infracciones, en tal sentido, Bermúdez, (2019) señala lo siguiente:

> En un estudio efectuado a 30 personas inmersas en el ejercer de derecho, se determinó que las principales falencias denotadas son la falta de socialización entorno a la comunidad sobre la existencia de las leyes y artículos penales afines a derechos informáticos que a pesar de existir denuncias no se toma enserio el caso o el delincuente sale libre por la falta de un debido proceso acorde al castigo legal (p. 9).

En el mismo sentido, se puede determinar que, dentro del Estado ecuatoriano, se han podido referenciar en porcentajes, los ciberdelitos que han sido objetos de investigación penal. Tal como a continuación se reflejan:

Tabla 1 Estadísticas de ciberdelitos en proceso de investigación año 2022 Ecuador

Delito	Porcentaje
Fraudes, estafas	54%
Robos con interceptación de dispositivos	40%
Pedofilia o acoso sexual	6%

Fuente: Campbell (2019)
Elaborado por: La investigadora

Es por lo expuesto que, se hace necesario mejorar las leyes nacionales en el ámbito de la informática, ya que se consideran insuficientes. Se enfatiza la importancia de proporcionar capacitación a autoridades locales, notarios y abogados. Esto se debe a que la población percibe que las Tecnologías de la Información y Comunicación (TIC) se han convertido en una poderosa herramienta para cometer infracciones legales.

No obstante, es relevante destacar que el problema fundamental no reside en las habilidades tecnológicas en sí, sino en la insuficiencia de recursos financieros para implementar medidas preventivas contra estos incidentes. Es evidente que las leyes no pueden adaptarse con la misma velocidad con la que surgen nuevos delitos informáticos. En este contexto, Ramos (2019) hace una observación al respecto:

> El derecho lamentablemente no estuvo preparado para combatir los aspectos negativos que trajo consigo la incidencia de la informática en la vida del ser humano, y aun cuando ya han pasado varios años desde su creación y evolución, la ciencia jurídica no ha podido descifrar muchos de los problemas que se presentan hoy en día (p. 18).

Para que se configure una estafa, en primer lugar, es necesario que haya un acto de engaño que resulte en una pérdida real o en la posibilidad de una pérdida en el patrimonio de la víctima. En este sentido, la estafa se considera un delito de naturaleza material, y puede ocurrir de manera incompleta. Por ejemplo, si alguien engaña con la intención evidente de causar daño económico, pero no lo logra debido a circunstancias fuera de su control, estaría cometiendo un delito de estafa frustrada.

A lo largo de un período considerable en Ecuador, se ha observado una progresiva evolución y complementación del texto legal. Esto se debe a que, hasta la reforma del 25 de junio de 1983, el código penal se refería principalmente a conceptos como defraudar, perjudicar y engañar. En esta interpretación particular de los delitos, convivieron diferentes objetivos y enfoques políticos relacionados con la criminalidad. En la actualidad, la norma penal, determina que Aquella persona que, con el propósito de obtener un beneficio económico para sí misma o para otra persona, emplee la falsificación de eventos falsos o la distorsión u ocultación de hechos verídicos, con el objetivo de engañar a alguien más y llevarlo a realizar una acción que cause daño a su patrimonio o al de una tercera persona, podría ser condenada a una pena privativa de libertad que va de cinco a siete años.

La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.
3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.
4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años (COIP, 2016, art. 186).

Si se comete una estafa a través de una entidad perteneciente al Sistema Financiero Nacional o de la economía popular y solidaria que realice actividades de intermediación financiera utilizando fondos privados, públicos o de la Seguridad Social, la sanción será una pena privativa de libertad que oscilará entre siete y diez años.

Aquel individuo que emita boletos o entradas para eventos en lugares públicos o de gran asistencia, superando el límite de capacidad autorizado por la autoridad pública competente, podría enfrentar una pena privativa de libertad de treinta a noventa días (Ortiz, 2019). Su conclusión, que resalta la necesidad de que cualquier delito esté claramente definido en la legislación vigente, es acertada. Es decir, todas las acciones que afecten la paz y la armonía de la sociedad deben estar reguladas por la ley, ya que no se pueden castigar mediante interpretaciones extensivas

Por lo tanto, es necesario establecer en la legislación nuevos tipos de delitos que sancionen las actividades ilegales emergentes como resultado del progreso tecnológico. Esto incluye delitos que se cometen en línea, como el ciberbullying, los ciberataques, las subastas y ventas ilegales en Internet, el uso de redes de robots o zombis, entre otros. Al respecto, Ortiz (2019) señala que:

> La incertidumbre del alcance: uno de los principales retos relacionados con el delito cibernético es la no existencia de información fehaciente sobre la trascendencia del problema y sobre las detenciones, los enjuiciamientos y las condenas correspondientes; sin esos antecedentes, es difícil cuantificar el impacto del delito cibernético en la sociedad y elaborar estrategias para combatirlo (p. 29).

Un gran aporte que hace García (2017) respecto a la estafa, es que, la estafa perpetrada a través de las redes sociales, al igual que la estafa convencional, se materializa cuando las personas son engañadas y dan su consentimiento para proporcionar información o creer en propuestas de negocio o entregas ofrecidas. Estas características fundamentales del delito se establecen de esta manera, por lo que no es apropiado clasificarla como un delito de apropiación fraudulenta mediante medios electrónicos o como una estafa común

Móviles de comisión de delitos

En primera instancia cabe hablar acerca del comercio, ya que, a través del mismo, se cometen la mayoría de los ciberdelitos en el mundo. Al respecto Vergara (2018) sostiene que:

> A principio de 1920 cuando apareció en EEUU la venta por catálogo, impulsado por empresas mayoristas. Este sistema de venta, revolucionario para la época, consistía en un catálogo con fotos ilustrativas de los productos a vender (p.65).

Esto estableció las directrices para un comercio a gran escala, permitiendo que los compradores realicen sus pedidos desde la comodidad de sus hogares. Esta forma de venta fue innovadora en ese período, y si la comparamos con el comercio electrónico que está en pleno auge en la actualidad, sigue manteniendo los mismos fundamentos Sin embargo, fue en los primeros años de la década de los 90 cuando se iniciaron las transacciones comerciales electrónicas. Según Alarcón (2017), se empezó a definir el comercio electrónico como la adquisición de bienes y servicios a través de la *World Wide Web* utilizando servidores seguros y empleando servicios de pago electrónico, como la autorización de tarjetas de crédito o billeteras electrónicas.

Fue solo a finales del siglo XX cuando se presenció el comienzo del comercio electrónico, con las primeras empresas que adoptaron Internet como un nuevo canal de ventas. En ese contexto, surgieron nuevas empresas como modelos de negocios alternativos, y aunque no fueron las pioneras, destacaron como las más exitosas hasta la fecha, incluyendo nombres como Amazon.com, eBay y otras (Chas, 2021).

Hoy en día, el comercio electrónico también se ha extendido al uso de plataformas móviles, gracias a la popularidad de los teléfonos móviles inteligentes, conocidos como '*smartphones*'. Además, en términos de opciones de pago, las transferencias bancarias y el reconocido PayPal son las alternativas más predominantes en la actualidad.

En ese sentido, Chas (2021) sostiene que Las personas tienen preferencia por estas transacciones debido a su inmediatez y rapidez, evitando así las tediosas esperas en filas. No obstante, es importante destacar que, si no se implementan medidas de seguridad adecuadas, estas operaciones pueden tener resultados lamentables. Las redes sociales han impulsado aún más el comercio electrónico, por lo que, el citado autor manifiesta:

> Es necesario describirlas como formas de interacción social, como un intercambio dinámico entre personas, grupos y organizaciones en diferentes contextos. Estas redes son herramientas de comunicación que

> proporcionan actualizaciones automáticas, perfiles visibles, capacidad de crear nuevos enlaces mediante servicios de presentación y otras maneras de conexión social en línea. Lo que ofrece a sus usuarios un lugar común para desarrollar comunicaciones constantes. La base del funcionamiento de las redes sociales es el mismo usuario puesto que las redes sociales son construidas y dirigidas por estos, quienes además constantemente las nutren de contenido (Chas, 2021, p. 17).

La velocidad con la que las redes sociales se actualizan las convierte en un entorno propicio para el crecimiento de las actividades comerciales y, como resultado, también para la aparición de oportunidades de ciberdelincuencia

Regulación del comercio electrónico

Con el surgimiento del comercio electrónico, se hace necesaria una normativa reguladora, por lo que, Chicarro (2019) determina:

> En 1995 se crea la Organización Mundial de Comercio (OMC), a fin de normar y regular los procesos de intercambio comercial entre los países. A pesar de que su injerencia todavía no es mundial, sentó las bases de la universalización de las transacciones comerciales, base fundamental del comercio electrónico (p. 26).

En el mismo sentido, dentro de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del Ecuador (2002) se determina:

> Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas (art. 2).

Los mensajes de datos serán legalmente equivalentes a los documentos escritos, y su validez, evaluación y consecuencias estarán sujetos al cumplimiento de las

disposiciones de esta ley y su reglamentación. Se otorga reconocimiento legal a la información que no está directamente incluida en un mensaje de datos, siempre y cuando aparezca en el mensaje de datos de manera referencial o adjunta a través de un enlace electrónico directo, y su contenido sea explícitamente conocido y aceptado por las partes involucradas.

Por lo que, el citado autor detalla que:

> El proceso de globalización en el que estamos inmersos llevó a las Naciones Unidas a la aprobación de una Ley Modelo y de una guía para su incorporación a los ordenamientos jurídicos internos de los diferentes países. El carácter gremial del derecho mercantil ha sido sustituido por un comercio electrónico de ámbito mundial (Chicharro, 2019, p. 19).

El avance de las tecnologías y la emergencia de los delitos informáticos hacen necesaria la creación de un campo legal especializado en estas cuestiones, así Dammert (2018) señala que:

> Se trata de una nueva área de estudio que interrelaciona el derecho con la tecnología, disciplina que generalmente se la denomina "Derecho Informático", "Derecho Telemático", "luscibernética", "Derecho de Internet", también "Derecho Tecnológico", "Derecho de las Nuevas Tecnologías de la Información y Comunicación TICS", o "Derecho de la Sociedad de la Información" (p. 189).

El análisis detallado del derecho informático se lleva a cabo mediante el entendimiento de sus principios y fundamentos, y se caracteriza por tener sus propios métodos e instituciones. La autonomía de esta nueva rama del derecho se deriva de sus características bien definidas en múltiples áreas. En el ámbito de la legislación, se ha promulgado una cantidad significativa de normativas específicas, tanto a nivel global como a nivel nacional en cada país que ha regulado este tema.

Procedimientos investigativos en la legislación ecuatoriana

Dentro del Estado ecuatoriano, el procedimiento penal, cuando de acción pública se trata, Fiscalía General del Estado, es el órgano regulador y encargado de titularizar las investigaciones previas, en el caso de los delitos cibernéticos o informáticos, la legislación ecuatoriana, los adentra con la vigencia del Código Orgánico Integral Penal en el año 2014. Así, EcuRed (2022) sostiene que:

> Cuando la ley se presentó en un principio, tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal de dicha ley, ya que las infracciones a la misma es decir los llamados delitos informáticos, como se los conoce, se sancionarían de conformidad a lo dispuesto en nuestro Código Penal, situación como comprenderán era un tanto forzada, esto si tomamos en cuenta los 65 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática, por tanto, les hacía inútiles por decirlo menos, para dar seguridad al Comercio Telemático ante el posible asedio de la criminalidad informática (p. 19).

De igual forma, en el año 2002 Ecuador, a través de su órgano legislativo, promulgó la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados delitos informáticos.

Actualmente, de acuerdo con Equipo de comunicaciones y Escuela de Seguridad Digital (2022) el Código Orgánico Integral Penal (2014) ha introducido una serie de delitos informáticos que no estaban previamente considerados. Los delitos informáticos o ciberdelitos son actos ilegales que se cometen empleando computadoras, sistemas informáticos u otros dispositivos de comunicación, donde la informática sirve como medio o herramienta para llevar a cabo la actividad delictiva.

Estos delitos pueden abarcar el robo de información, la apropiación de contraseñas, el fraude en cuentas bancarias y otras acciones similares.

Desde que el Código Orgánico Integral Penal entró en vigor en 2014, incluye y penaliza los delitos informáticos, que abarcan acciones como la divulgación ilegal de bases de datos, la interceptación no autorizada de información, la transferencia electrónica de fondos obtenidos de manera ilícita, los ataques contra la integridad de sistemas informáticos, el acceso no autorizado a sistemas telemáticos o de telecomunicaciones, la producción y distribución de pornografía infantil y el acoso sexual.

La Policía Nacional del Ecuador, refiere a los ciudadanos que deben denunciar todos estos actos cibernéticos, así pueden acercarse a cualquier centro de atención ciudadana, en los servicios de atención integral (SAI). Estos centros se encuentran dentro de las instalaciones de la Fiscalía General del Estado, de cualquier cantón o ciudad a lo largo del territorio ecuatoriano.

Cada vez más personas optan por realizar transacciones financieras en línea. Estas transacciones son instantáneas y eficientes, evitando largas esperas en filas. Sin embargo, es crucial tomar medidas de seguridad para evitar consecuencias adversas. Es fundamental abstenerse de ingresar información confidencial, como contraseñas y números de tarjeta, en redes públicas, como cibercafés o centros comerciales. Mantener el sistema operativo actualizado es esencial para evitar posibles vulnerabilidades de seguridad. Además, es recomendable emplear contraseñas únicas para cada sitio, como correo electrónico y cuentas bancarias, con el fin de fortalecer la seguridad.

En ese sentido, Herrero (2017) señala que es imprescindible contar con un software antivirus actualizado que incluya un sistema de control de navegación en Internet es fundamental. Cambiar las contraseñas regularmente es una práctica recomendada. Es esencial verificar siempre que se trata de una página segura, identificada por "https". Evitar hacer clic en enlaces sospechosos o recibir correos electrónicos de fuentes no

confiables es una medida de precaución importante. Además, es relevante destacar que la Dirección Nacional de Comunicaciones, a través de su Área de Seguridad de la Información, está implementando el proyecto del Esquema Gubernamental de Seguridad de la Información. El objetivo de este proyecto es asegurar la disponibilidad, confidencialidad e integridad de la información de la Policía Nacional de Ecuador.

Métodos de investigación para ciberdelitos en el Ecuador

Las organizaciones supranacionales también han experimentado interrupciones debido a delitos cibernéticos de naturaleza política o ideológica, así como ciberataques, *hacktivismo* y *ciberterrorismo*. Para Vergara (2018) estas actividades se han empleado para desestabilizar un Estado o difundir mensajes políticos, aprovechando la amplia difusión que ofrece el ciberespacio. Los ataques de denegación de servicio, infecciones de malware y otras acciones similares siguen perturbando las operaciones de instituciones importantes en un país, causando daños significativos, incluyendo pérdidas económicas.

Efectivamente, el ciberdelito se ha convertido en una de las amenazas más significativas para la economía global. Para las empresas, los costos y las pérdidas asociadas a los delitos cibernéticos son inmensos e incluyen aspectos como la corrupción, la destrucción de datos, el robo de fondos, la apropiación indebida de propiedad intelectual, datos personales y financieros, así como la interrupción de las operaciones comerciales después de un ciberataque. Además, Larios (2018) esto puede ocasionar daños a la reputación corporativa, pérdida de productividad, entre otros. Los datos disponibles respaldan estas inquietudes. De acuerdo con un informe reciente del Banco Interamericano de Desarrollo, se estima que los daños causados por los delitos cibernéticos alcanzarán los seis billones de dólares para el año 2021, lo que equivale al Producto Interno Bruto (PIB) de la tercera economía más grande del mundo.

Lucha contra la ciberdelincuencia

La seguridad es un recurso público que puede verse amenazado por la actividad delictiva. En la actualidad, la seguridad no solo en el mundo físico, sino también en el ámbito digital, se considera un valor que debe ser garantizado. Por lo tanto, reconociendo la importancia de establecer regulaciones que faciliten la lucha efectiva contra los delitos informáticos, el Estado ecuatoriano, en su Constitución, asume la responsabilidad de formular políticas destinadas a proteger los derechos de las personas, incluyendo la protección del ciberespacio. En este contexto, en Ecuador, los ciberdelitos están definidos y castigados en el Código Orgánico Integral Penal de 2014, como un enfoque para combatirlos y establecer sanciones correspondientes.

Desde la implementación del Código Orgánico Integral Penal (2014), el Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado ha experimentado un aumento notable en la cantidad de denuncias relacionadas con este tipo de delitos. Específicamente, el aumento de denuncias se centra en delitos como el contacto con menores de dieciocho años por medios electrónicos con propósitos sexuales, entre otros. En ese sentido, es preciso detallar cuantas denuncias se han presentado en este contexto desde el año 2014 hasta el año 2020:

Tabla 2 Número de denuncias entre 2014-2019 Ecuador.

Delito	Número de denuncias entre el 2014-2019
CHILD GROOMING	829
APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	10.393
TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL	387
ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES	829

Elaborado por: El investigador
Fuente: Fiscalía General del Estado (2023).

Para abordar eficazmente el ciberdelito, es esencial comprender su origen, sus causas, motivaciones y la diversidad de personas involucradas. Esto implica la formulación de políticas tanto a nivel nacional como empresarial, así como la adopción de medidas a nivel individual. Además, se requiere el desarrollo de herramientas y tecnologías que permitan a los usuarios ejercer su derecho a protegerse de manera práctica. En este contexto, la adecuación del derecho penal desempeña un papel crucial en el procesamiento de delitos cibernéticos, ya sea a nivel nacional o internacional.

No obstante, con frecuencia, las nuevas formas de actividad delictiva relacionadas con el ciberdelito han expuesto las restricciones de las instituciones creadas para garantizar la seguridad nacional y la aplicación de la ley. En realidad, el ciberdelito representa una amenaza significativa que presenta numerosos obstáculos para el sistema de derecho penal convencional y el sistema de justicia en su totalidad.

1.2. Tutela judicial efectiva

Tutela judicial efectiva, definiciones, elementos, características, naturaleza jurídica y alcance de protección normativa.

No se puede pasar por alto el acontecimiento crucial que marcó el precedente fundamental para la tutela judicial efectiva en los Tribunales Europeos. Durante la década de 1940, los derechos fundamentales de las personas eran prácticamente ignorados en esa región, especialmente durante la Segunda Guerra Mundial, un periodo histórico caracterizado por la progresiva vulneración de los derechos inherentes a la humanidad. Sin embargo, al término de este conflicto, se generó una conciencia significativa en los Estados respecto a la necesidad de establecer mecanismos efectivos para la protección de los derechos fundamentales.

En este contexto surge la tutela judicial efectiva, como lo describe Lemaitre (2020): "Con el derecho fundamental a la tutela judicial efectiva, el derecho europeo, seguido por los organismos internacionales de la Comunidad Europea, busca ampliar la esfera de garantías de los derechos e intereses legítimos de las personas" (p. 19). Similar a otros derechos, la tutela judicial efectiva surge como una imperiosa necesidad de salvaguardar a los ciudadanos frente al poder estatal, al mismo tiempo que constituye una respuesta al deber del Estado de proteger los derechos fundamentales de las personas.

En este sentido, la tutela judicial efectiva viene a convertirse en un reto para los estados europeos, que bien pudo haber desaparecido por el autoritarismo que en aquella época predominaba, o bien seguirse ampliando en contenido como hasta la actualidad. De igual manera, el citado autor, indica como antecedente lo siguiente:

> La Ley Fundamental de Bonn de 1949, en su artículo 19 (IV), estableció el derecho fundamental individual a la tutela judicial efectiva, considerado como un derecho general de libertad y como la coronación del Estado de derecho, pues comprende el derecho procedimental básico cuyo propósito principal fue ampliar el conjunto de garantías procesales, es decir el derecho de acceso a la jurisdicción y el debido proceso para comprender la justiciabilidad de los conflictos que se originan entre los ciudadanos y los poderes públicos, y con ello el control judicial efectivo frente al ejercicio del poder público, principalmente de la administración, con lo cual el derecho a la tutela judicial efectiva en Alemania se dirige principalmente a enjuiciar la actuación administrativa, mientras que los litigios que se deducen de las relaciones jurídicas privadas y de los procesos penales se fundan en la cláusula del Estado de Derecho (p. 20).

Puede afirmarse que, en Alemania, la tutela judicial efectiva tiene su origen como una garantía fundamental destinada a resguardar a las personas de posibles abusos por parte del poder estatal. Posteriormente, evoluciona para incluir en su ámbito de aplicación las relaciones jurídicas entre individuos. Se sostiene, por lo tanto, que la

tutela judicial efectiva engloba el derecho de acceso a la jurisdicción y al debido proceso, asegurando así los derechos de los justiciables frente a cualquier procedimiento judicial.

El contenido de la tutela judicial efectiva ha sido desarrollado también en gran abundancia por el Tribunal Constitucional español, dotándole a este derecho de numerosos atributos, a partir de que la Constitución española de 1978 en su artículo 24 estableció:

> Todas las personas tienen derecho a obtener tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión. 2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia. La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos (p. 19).

La Constitución española refleja que el derecho de acceso a la justicia no se limita únicamente a la posibilidad de recurrir a los órganos jurisdiccionales para reclamar la protección de un derecho infringido, sino que también implica la comprensión de que la tutela judicial efectiva está intrínsecamente vinculada a otros derechos, como el debido proceso.

Desde sus inicios, la tutela judicial efectiva y el debido proceso coexisten de manera indivisible, dando lugar a la obtención de respuestas plenamente fundamentadas en las pretensiones de las partes involucradas. En este sentido, Chamorro (2021) presenta la siguiente perspectiva:

> A partir del art. 24.1, el concepto tutela judicial efectiva supuso una auténtica revolución en el ámbito jurídico y en especial en el derecho procesal, todo ello a lo largo de un paciente desarrollo jurisprudencial que ha determinado el ámbito de las garantías constitucionales derivadas de este derecho, haciendo “chirriar” muchas veces las estructuras mismas de la administración de justicia (p. 22).

El escritor reconoce que a partir de lo establecido en el artículo 24.1 de la Constitución Española de 1978, se originan importantes precedentes que van delineando los componentes fundamentales de la tutela judicial efectiva tanto en el ámbito procesal como en el constitucional. Esta evolución inevitablemente conducirá a cambios significativos en la administración de justicia, ya que se deberá elegir métodos apropiados para que esta función estatal garantice de manera efectiva la protección del derecho a la tutela judicial.

La tutela judicial efectiva como un derecho fundamental

Actualmente, con la vigencia de la Constitución de 2008, se percibe que esta proporciona derechos más amplios para la ciudadanía, presentando un catálogo muy extenso. Se destaca que ninguna acción en este ámbito debe llevarse a cabo de manera arbitraria, evidenciando así que los derechos fundamentales están destinados a limitar los poderes estatales, actuando como un contrapeso contra la arbitrariedad estatal.

La norma constitucional, al establecer características comunes de los derechos y principios, señala que "Todos los principios y los derechos son inalienables, irrenunciables, indivisibles, interdependientes y de igual jerarquía" (p. 69). A partir de esta disposición, se comprende que tanto los principios como los derechos tienen igual jerarquía y, por lo tanto, se debe exigir su cumplimiento y observancia de manera equitativa.

En este contexto, se puede afirmar que los derechos fundamentales se derivan de la Norma Fundamental de cada Estado, es decir, de las Constituciones. Además, se destaca que los derechos fundamentales son inherentes a la naturaleza humana, siendo intrínsecos a cada individuo, a cada ciudadano, no solo por pertenecer a un determinado territorio, sino más bien por el simple hecho de ser y, además que constituyen el límite a los abusos de poder.

Otra definición bastante interesante es la que nos presenta Benavides (2022) quien señala:

> De tal modo que podemos entender por derechos fundamentales a aquellos derechos subjetivos que le son propios a la persona en cuanto tal, que por la importancia de los bienes jurídicos que representan, tienen reconocimiento constitucional, de ahí que de dicho reconocimiento se derivan consecuencias de tipo jurídico, tales como la tutela judicial efectiva y el contenido esencial (p. 17).

En este sentido, los derechos fundamentales siempre estarán dirigidos a las personas por su naturaleza como tal, los mismos que son totalmente exigibles el momento en el cual se vulnere su contenido esencial o se encuentre en amenaza, es decir que los derechos fundamentales no yacen por sí solos, los mismos contienen elementos que a simple vista no son identificables, pero conforme el desarrollo jurisprudencial y el actuar mismo del ser humanos en sociedad permiten establecerlos para poder generar mejores mecanismos de protección. Para autores como Robert Alexy (1996), surge la necesidad de distinguir a la norma de derecho fundamental y el derecho fundamental, así se precisa lo siguiente:

> Entre el concepto de norma de derecho fundamental y el de derecho fundamental existen estrechas conexiones. Siempre que alguien posee un derecho fundamental, existe una norma válida de derecho fundamental que le otorga este derecho. Es dudoso que valga lo inverso. No vale cuando existen normas de derecho fundamental que no otorgan ningún derecho subjetivo (p. 71).

El autor mencionado previamente argumenta que, aunque derecho fundamental y norma de derecho fundamental no sean conceptos idénticos, estos elementos guardan una relación entre sí. Esto se debe a que los derechos fundamentales representan derechos subjetivos en sí mismos, y estos derechos subjetivos deben estar contemplados en normativas para su exigibilidad y cumplimiento. En este sentido, la Norma Fundamental de cada Estado es la que recoge el contenido de las normas de derecho fundamental, estableciendo así las normativas que regulan los derechos inherentes al ser humano.

Cuando se aplica esta teoría al tema de la presente investigación, se comprende que la tutela judicial efectiva, al ser tratada como un derecho fundamental, debe garantizarse de manera incondicional, ya que constituye un derecho arraigado a la condición humana. Además, se destaca que este derecho debe contar con garantías específicas para su protección, con el propósito de prevenir consecuencias jurídicas significativas y graves para el justiciable. Estas consideraciones permiten entender que la tutela judicial efectiva también desempeña un papel fundamental para evitar abusos por parte de la actividad jurisdiccional hacia los ciudadanos, asegurando que las causas sean tramitadas de manera legal y adecuada, sin alterar la naturaleza del conflicto que se somete a la decisión de los jueces.

La teoría analizada anteriormente trasladada al tema de la presente investigación nos permite comprender que la tutela judicial efectiva al ser tratada como derecho fundamental, debe garantizarse sin excepción alguna; ya que, constituye un derecho arraigado a la condición humana. Además, que el mismo debe contar con garantías que se enfoquen en su protección y en el hecho de evitar consecuencias jurídicas relevantes y graves para el justiciable. Estas consideraciones, permiten entender que también la tutela judicial efectiva cumple su función para que no existan abusos por parte de la actividad jurisdiccional hacia los ciudadanos y que sus causas sean tramitadas en legal y debida forma sin alterar la naturaleza del conflicto que se somete a la decisión de los jueces.

La tutela judicial efectiva como un medio de justicia

Los elementos que integran la tutela judicial efectiva, son elementos que constituyen la dimensión procesal del derecho, por lo tanto, no es de sorprenderse que en nuestra legislación se haya tomado en cuenta a la tutela judicial efectiva como principio de la actividad jurisdiccional. La labor de administrar justicia constitucional exige una gran comprensión primero de lo que involucra en una dirección general la administración de justicia como tal y como esta actividad debe desenvolverse en pro de los justiciables, para lo cual dicha actividad deberá estar regida por principios que coadyuven a la vigencia plena de los fines de la administración de justicia.

Como bien lo indica Meléndez (2018): “La función jurisdiccional del Estado, como importante actividad humana que es, no escapa a estas consideraciones y tiene entonces también principios que le inspiran (p. 67). Así, se comprende que, la tutela judicial efectiva trasladada como principio de carácter procesal da la posibilidad de dirigir la actividad de administrar justicia, tal es el caso que algunas legislaciones incluida la nuestra en la norma que regula la actividad judicial la desglosa como principio, ya que la misma debe ser observada en todo momento del proceso y dirigir el mismo en virtud de su contenido esencial antes ya analizado.

En la legislación ecuatoriano dentro del artículo 23 del Código Orgánico de la Función Judicial (2009) se define a la tutela judicial efectiva como:

> La Función Judicial, por intermedio de las juezas y jueces, tiene el deber fundamental de garantizar la tutela judicial efectiva de los derechos declarados en la Constitución y en los instrumentos internacionales de derechos humanos o establecidos en las leyes, cuando sean reclamados por sus titulares o quienes invoquen esa calidad, cualquiera sea la materia, el derecho o la garantía exigido. Deberán resolver siempre las pretensiones y excepciones que hayan deducido los litigantes sobre la única base de la Constitución, los instrumentos internacionales de

> derechos humanos, los instrumentos internacionales ratificados por el Estado, la ley, y los méritos del proceso (art. 23).

Es por lo que, se entiende que, la función judicial cumple su rol a través de los jueces en sus diferentes competencias generadas por ley, pues así mismo se debe comprender que la tutela judicial efectiva al ser considerado un principio procesal para la administración de justicia dirige dicha actividad y la misma no debe ser comprendida como una mera formalidad que nos limita a pensar que al vulnerar los derechos que constituyen su contenido esencial de no es vulnerar el principio de tutela judicial efectiva.

Cabe señalar que así la vulneración sea en conjunto o de manera singular a estos derechos estamos hablando de vulneración a la tutela judicial efectiva; pues no podemos comprender su contenido esencial de manera distante. Diremos entonces, que la tutela judicial efectiva tomada como un principio procesal exige a las autoridades capaces de administrar justicia su observancia durante todo el proceso incluyendo la ejecución de la decisión que se haya tomado respecto de la causa sometida a su conocimiento, sin menoscabar derecho alguno que constituye su contenido fundamental.

La tutela judicial efectiva desde la legislación ecuatoriana

El Ecuador, al igual que el resto de los países incluidos en el Sistema Interamericano de Derechos Humanos, tiene la obligación de acoger las disposiciones emanadas de la Corte IDH y demás organismos internacionales, es así que, a partir de este precepto, partimos de la norma constitucional, analizando el contenido mismo del derecho a la tutela judicial efectiva, precisando que el artículo 75 de la Constitución de la República del Ecuador (2008), prescribe:

> “Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en

> indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley (art. 75).

Lo que permite comprender a simple vista que, la tutela judicial efectiva a más de permitir el acceso al órgano jurisdiccional permite la efectividad de las decisiones judiciales. El derecho a la tutela judicial efectiva se encuentra especificado como una obligación de los operadores de justicia, así dicho derecho se encuentra determinado en el artículo 15 del Código Orgánico de la Función Judicial (2009), que reza lo siguiente: “El Estado será responsable en los casos de error judicial, detención arbitraria, retardo injustificado o inadecuada administración de justicia, violación del derecho a la tutela judicial efectiva, y por las violaciones de los principios y reglas del debido proceso” (art.),39 en el . Este artículo la tutela judicial efectiva aparece como una obligatoriedad estatal, ya que el Estado es el responsable de mantener vigente este derecho a través de sus actuaciones y el mismo debe propender por mecanismos sumamente fuertes para evitar su vulneración.

En tal sentido, en Ecuador también se resalta el carácter prestacional que posee la tutela judicial efectiva frente al ciudadano. Por otro lado, en la misma norma aparece como un principio en el artículo 23 del Código Orgánico de la Función Judicial (2009), a fin de optimizar la actuación jurisdiccional, indicándose:

> La Función Judicial, por intermedio de las juezas y jueces, tiene el deber fundamental de garantizar la tutela judicial efectiva de los derechos declarados en la Constitución y en los instrumentos internacionales de derechos humanos o establecidos en las leyes, cuando sean reclamados por sus titulares o quienes invoquen esa calidad, cualquiera sea la materia, el derecho o la garantía exigido (art. 23).

Al constituirse como principio, los funcionarios que pertenecen a la función judicial no deberán omitir la observancia de este contenido, ya que el mismo se encuentra establecido a más de derecho como principio, con la finalidad de que los derechos de

los ciudadanos frente a la administración de justicia no sean soslayados desde el momento mismo en el que se da inicio a la acción judicial, abarcando el desarrollo del proceso, hasta su finalización con una decisión y posterior ejecución de dicha decisión.

La tutela judicial efectiva desde la jurisprudencia

Cualquier intento de vulneración o la vulneración misma del derecho a la tutela judicial efectiva será sancionado, en aras de salvaguardar la vigencia del Estado constitucional de derechos y justicia proclamada en nuestra norma suprema, lo cual implica la observancia de los derechos fundamentales de los ciudadanos sin restricción alguna. Con relación a la tutela judicial efectiva y su contenido esencial, nuestra Corte Constitucional (2020) sostiene lo siguiente:

> El derecho a la tutela efectiva, imparcial y expedita de los derechos de las personas tiene relación con el derecho de acceso a los órganos jurisdiccionales para que, luego de un proceso que observe las garantías mínimas establecidas en la Constitución y la ley, se haga justicia; por tanto, se puede afirmar que su contenido es amplio y en éste se diferencian tres momentos: el primero relacionado con el acceso a la justicia, el segundo con el desarrollo del proceso en un tiempo razonable, y el tercero que tiene relación con 40 Ibíd. 41 la ejecución de la sentencia, esto es, acceso a la jurisdicción, debido proceso y eficacia de la sentencia (Sentencia N.° 030-10-SCN-CC, caso N.° 0056-10-CN, 10 de marzo de 2014).

De la decisión citada por la Corte Constitucional, se puede identificar que la tutela judicial efectiva debe manifestarse en sus tres momentos de manera activa, tanto al inicio del proceso con la acción, durante el proceso y la etapa de ejecución, tomando en consideración el tiempo razonable, tal cual, como señala también la Corte IDH.

Sin embargo, en la evaluación práctica se encuentra frente a una y otra garantía jurisdiccional que alega la vulneración del derecho a la tutela judicial efectiva en cualquiera de estas etapas, lo cual, permite inferir que la tutela judicial efectiva al ser

un derecho general debe ser observada desde su contenido en su totalidad ya que la vulneración de una etapa del proceso al igual que todas las etapas del proceso, constituiría vulneración a la tutela judicial efectiva.

La Corte Constitucional del Ecuador, ha señalado:

> La tutela judicial efectiva garantiza a las personas el acceso a la justicia, sin que su pleno ejercicio se agote únicamente en la posibilidad de acudir a los órganos jurisdiccionales, pues implica también la obligación que tiene el operador de justicia de sustanciar la causa observando el procedimiento establecido por el ordenamiento jurídico para cada caso y concluyendo el mismo a través de una decisión motivada que garantice los derechos de las partes y que deberá ejecutarse adecuadamente dentro del marco jurídico aplicable (Sentencia N.° 030-10-SCN-CC, caso N.° 0056-10-CN, 10 de marzo de 2014).

Entonces, la Corte Constitucional ha sido muy clara en establecer la obligatoriedad que recae sobre el órgano jurisdiccional de mantener la observancia de este derecho, indicándonos que tutela judicial efectiva no termina con el simple hecho de acudir al órgano jurisdiccional, sino que es a partir de allí donde empieza a manifestarse este derecho, enfocándose en la sustanciación del proceso según el procedimiento normado para cada caso e incluyendo que sus decisiones sean motivadas y la ejecución de las mismas como parte del contenido de la tutela judicial efectiva.

La Corte Constitucional más adelante siguiendo su línea jurisprudencial, ha demarcado de manera muy clara cuales son los aspectos que conforman la tutela judicial efectiva, indicando lo siguiente: “En este contexto, la Corte Constitucional ha desarrollado el contenido de la tutela judicial efectiva y al hacerlo ha sostenido consistentemente que esta se compone de tres supuestos, a saber: 1. el acceso a la administración de justicia” (Sentencia N.° 015-16-SEP-CC, caso N.° 1112-15-EP, 13 de enero del 2016). La observancia de la debida diligencia; y, 3. la ejecución de la decisión. Como parte de la tutela judicial efectiva, reconoce a las partes el derecho a obtener una solución

al conflicto, esto es una sentencia que resuelva sobre el fondo de la controversia de manera motivada.

En este sentido, la Corte Constitucional ha precisado tres elementos que conforman la tutela judicial efectiva, dejando claro la complejidad de este derecho y la comprensión obligatoria de su contenido. Entonces, para hablar de vulneración a la tutela judicial efectiva, debemos aterrizar en los tres elementos claramente establecidos en la realidad ecuatoriana, los cuales serán descritos a continuación. El primer elemento es el acceso a la administración de justicia, la tutela judicial efectiva no solo se refiere al acceso al órgano judicial, sino que este aspecto forma parte en sí de la tutela judicial efectiva. Entonces será necesario que el Estado proceda a establecer mecanismos suficientes que amparen y garanticen el acceso al a la administración de justicia a todas las personas, sin excepción alguna, con la finalidad de hacer valer sus derechos; sin embargo, hasta ahí no se constituye la tutela judicial efectiva, este derecho o garantía va tomando forma durante el desenvolvimiento del proceso, hasta su finalización. En relación al acceso a la administración de justicia la Corte Constitucional en el caso No. 1209-14-EP, realiza un análisis respecto a una Acción Extraordinaria de Protección presentada, partiendo del primer componente de la tutela judicial efectiva, la Corte Constitucional entonces menciona:

> El primer elemento relacionado a la tutela judicial efectiva se cumplió en el caso, toda vez que el legitimado activo pudo acceder al sistema de administración de justicia, de manera directa, sin encontrar trabas u obstáculos insubsanables; por lo que este primer elemento fue garantizado" (Sentencia N.° 1943-12-EP/19, caso No. 1943-12-EP, 25 de septiembre del 2019).

Por lo tanto, el primer elemento de la tutela judicial efectiva permite que quienes necesiten acceder a los órganos jurisdiccionales no tengan ningún tipo de inconveniente al hacerlo; en este sentido, se resalta entonces la obligación que tiene el Estado ecuatoriano de brindar los mecanismos necesarios para garantizar este acceso, evitando así la limitación al goce de este derecho. Como segundo elemento

se encuentra la observancia de la debida diligencia, el mismo que se refiere a cómo el administrador de justicia debe tramitar las causas puestas en su conocimiento, en observancia de las normas constitucionales vigentes y las normas específicas aplicables a los diferentes casos.

Para este segundo elemento, la Constitución de la República del Ecuador (2008), ha indicado en el segundo inciso del artículo 172, lo siguiente: “Las servidoras y servidores judiciales, que incluyen a juezas y jueces, y los otros operadores de justicia, aplicarán el principio de la debida diligencia en los procesos de administración de justicia” (art. 172). Entonces la debida diligencia viene a constituirse como un principio rector de la administración de justicia, y su observancia es de manera obligatoria por todos los operadores de justicia.

La Corte Constitucional del Ecuador refiere lo siguiente:

> Por su parte, de acuerdo con el segundo parámetro, los operadores de justicia deben actuar con sujeción al principio de la debida diligencia para resolver el caso puesto a su conocimiento. La "debida diligencia", se refiere a la actuación pronta y prolija por parte de las autoridades jurisdiccionales; esto es, en un tiempo razonable y dando trámite a la causa con apego a la normativa pertinente, con el objeto de dar efectiva protección a los derechos e intereses de las partes (Sentencia” N.° 364-16-SEP-CC, caso N.° 1470-14-EP, 15 de noviembre del 2016).

De lo mencionado por la Corte Constitucional, se revisa que, las causas deberán ser tramitadas entonces en observancia de las normas previamente establecidas y que sean aplicables al caso que ha de resolverse, pues la conducta del juzgador en cada caso deberá tener un mismo patrón de prontitud y prolijidad, además que deberá observarse la naturaleza de cada caso que se podrá en su conocimiento, ya que habrán causas que requieran un tratamiento especial y más célere respecto a otras causas.

Entonces, como parte de la debida diligencia se tiene al tiempo razonable, a la conducta del juzgador frente a los casos puestos en su conocimiento, a la tramitación de acuerdo a las normas aplicables al caso, sin embargo, más adelante la Corte Constitucional vendrá a precisar que no solo de estas observancias se nutre la debida diligencia, sino también se incluye al debido proceso, así en el caso 1234-14-EP, se explica lo siguiente:

> La debida diligencia implica que los juzgadores tienen la obligación de observar las garantías del debido proceso y actuar de forma cuidadosa en la tramitación de las causas puestas a su conocimiento; de modo que, deben velar porque en todo proceso las personas reciban una respuesta oportuna a través del ejercicio de las garantías mínimas previstas en la CRE (Sentencia N.° 1234-14-EP/20, caso N.° 1234-14-EP, 11 de marzo del 2020).

Se debe comprender que, el parámetro de debida diligencia implica de igual manera la observancia de las garantías mínimas que deben tomarse en cuenta siempre en la tramitación de todos los procesos judiciales, esto es el debido proceso, además que cada caso debe ser resuelto conforme las normas vigentes en el ordenamiento jurídico ecuatoriano.

Es de vital importancia que la administración de justicia a través de sus órganos jurisdiccionales logre materializar la protección de los derechos de la ciudadanía, tomando en cuenta cada parámetro fijado para mejor tramitar y resolver, la vulneración de uno o de varios componentes de la debida diligencia trae consigo la vulneración de la tutela judicial efectiva.

El último elemento que constituye la Corte Constitucional como parte de la tutela judicial efectiva es la ejecución de la decisión, en relación a este parámetro es necesario establecer que un proceso judicial no finaliza siempre con el establecimiento de una sentencia, pues la misma puede ser sujeta de recursos sean estos horizontales o verticales y a más de ser fundamentada deberá estar constituida por obligaciones de

hacer o no hacer en relación a cada caso concreto y dichas obligaciones deben ser acatadas por quienes accedan al órgano judicial independientemente del rol que vayan a desempeñar dentro del proceso judicial, es decir que se llegue a resarcir el derecho que haya sido vulnerado o del cual se exige su cumplimiento.

Así, por ejemplo, en relación a las garantías jurisdiccionales, se tiene que una acción que permite hacer efectivo el cumplimiento de las decisiones judiciales en materia de garantías, la misma que se denomina acción de incumplimiento de sentencias y dictámenes constitucionales, para lo cual la Corte Constitucional, ha establecido lo siguiente:

> Los procesos judiciales solo terminan con la aplicación íntegra de la sentencia o la reparación integral del derecho vulnerado; en otras palabras, gracias a esta garantía, los procesos constitucionales no llegan a su fin con la expedición de la sentencia, sino cuando haya cumplido con todos los actos que se haya dispuesto en ella y se ha llevado a cabo la reparación integral de los derechos vulnerados, tarea que además le corresponde a la Corte vigilar conforme sus atribuciones (Sentencia N.° 002-13-SIS-CC, caso N.° 00047-10-IS, 18 de septiembre del 2013).

A través de la mencionada disposición constitucional se insta entonces a la administración de justicia que no solo será necesario con el establecimiento de una sentencia para dar por finalizado el proceso judicial, sino que la misma debe cumplirse y acatarse, además que el juez deberá tener a la mano las herramientas necesarias para hacer cumplir dichas disposiciones, en aras de salvaguardar el derecho de quién ha reclamado y dicha disposición haya sido emanada a su favor.

Es necesario señalar que se puede encontrar casos en los cuales, de existir una sentencia con ciertas obligaciones para las partes procesales, las mismas pueden ser impugnadas a través de los recursos que prevé la ley y se suspende su ejecución mientras se resuelve la impugnación efectuada por cualquiera de las partes procesales o ambas partes procesales.

Así mismo, existen sentencias donde la ejecución de la misma no se suspende por el hecho de haberla impugnado, este es el caso de las garantías jurisdiccionales, pues el cumplimiento de estas sentencias es de carácter inmediato. Una vez analizado el componente de la tutela judicial efectiva según la Corte Constitucional en Ecuador, es necesario abordar el contenido doctrinario en cuanto a este derecho, así la doctrina procesal ecuatoriana también se ha encargado de generar el contenido esencial del derecho a la tutela judicial efectiva, al respecto la autora Aguirre (2021), permite conocer de manera más específica los elementos constitutivos de este derecho, los cuales son: “derecho de acceso a la justicia, defensa en el proceso, el derecho de una resolución motivada y congruente y el derecho a la efectividad de las decisiones jurisdiccionales, pues sin que concurran estos elementos no podemos hablar de tutela judicial efectiva” (p. 49).

No se puede dejar de evaluar también cuál es el sentido que le da el Estado ecuatoriano a este derecho, si se mantiene como un derecho específico del sistema procesal o si este se desenvuelve como derecho fundamental, al respecto, es decir, que la tutela judicial efectiva comparte de las dos aristas, ya que al ser un derecho fundamental este debe estar concretizado en cada una de las normativas que amparan el acceso a la justicia y que determinan el actuar de la administración de la función jurisdiccional.

De la lectura del texto de la autora Ochoa (2021), también se enfatiza que: “En la perspectiva del efecto irradiante que le incumbe como derecho fundamental, la tutela judicial efectiva se proyecta también en la interpretación y aplicación de las normas por los tribunales” (p. 50).

Al respecto, se considera que, tanto la interpretación como la aplicación de las normas, también constituyen parte de la tutela judicial efectiva, ya que por medio de esta actividad se está garantizando el deber que posee el juez frente a los ciudadanos para precautelar sus intereses en igualdad de condiciones, al revisar la norma que más se

apegue al caso para resolverlo, ya que se cuenta con un principio de seguridad jurídica que permite la existencia de normas jurídicas previas y claras.

No cabe ninguna duda entonces, que la tutela judicial efectiva viene a presentarse como aquel derecho protector de otros derechos que tienen los ciudadanos frente a la administración de justicia, ya que por un lado las pretensiones que emanen de los justiciables constituyen la razón de existencia de la función jurisdiccional en cada Estado y por otro lado los ciudadanos se encuentran al amparo de que el contenido axiológico de la actividad jurisdiccional sea materializado, es decir, la Justicia.

Por tal motivo se hace necesaria la obligatoriedad de los estados de crear varios mecanismos efectivos encaminados a la protección de los derechos fundamentales de sus ciudadanos. En este sentido, Colombia se presenta al derecho de tutela judicial efectiva como una garantía primordial del Estado, partiendo de su contenido prestacional al amparo de todos los ciudadanos del país, Perú se centra en la arista procesalista, al tratar de equiparar la tutela judicial efectiva y debido proceso; y, por otro lado Ecuador se presenta como un país que reconoce al derecho a la tutela judicial efectiva en dos dimensiones totalmente marcadas, por un lado como garantía y por otro como principio procesal de la actividad judicial. Sin embargo, esta consideración se vuelve no tan necesaria cuando se trata de observar que cada una de las legislaciones analizadas consideran cada elemento que contiene la tutela judicial efectiva el acceso al órgano jurisdiccional, lo cual involucra tener jueces independientes, la observancia de los derechos del debido proceso desde el inicio de la acción, hasta su finalización y posterior ejecución.

1.3. Procesos investigativos en el Ecuador para ciberdelitos como medios de tutela judicial efectiva

Ecuador muestra su interés en recibir apoyo para la incorporación de procedimientos, así como para actividades de prevención y colaboración internacional relacionadas con la Convención de Budapest (2021) y la Convención de las Naciones Unidas contra el ciberdelito (2001). Adicionalmente, sería de gran utilidad recibir orientación en la

elaboración de manuales, instrucciones y directrices para el manejo de pruebas digitales, así como respaldo legal y técnico para establecer y poner en funcionamiento el Centro de Seguridad Cibernética de la Policía Nacional.
Dentro de un informe que realiza el Ministerio del Interior del Ecuador del año 2022, dirigido para las Naciones Unidas, determina que es importante fortalecer áreas dentro de la investigación que se especialicen en las siguientes ramas:

a) Análisis estadístico y dinámico de códigos maliciosos
b) Análisis y estudios criptográficos
c) Análisis forense de servidores
d) Análisis forense de infraestructuras híper convergentes
e) Análisis forense en Sistemas Operativos Windows, Linux y Ios
f) Análisis forense en dispositivos de almacenamiento
g) Análisis de Malware
h) Aplicación de la ciencia forense en los delitos informáticos y su punibilidad
i) Aplicación del derecho sustantivo y procesal, así como sobre solicitudes y prestaciones de asistencia judicial recíproca en materia penal en temas vinculados al ciberdelito (P. 2).

Estos aspectos son fundamentales para que los agentes investigadores del Ecuador, puedan contribuir a Fiscalía General del Estado de manera eficaz cuando se encuentren frente a un ciberdelito, estas especializaciones son de vital importancia para que las investigaciones puedan ser llevadas a juicio y, a posteriori, puedan terminar en una sentencia condenatoria en donde se repare a la víctima su derecho vulnerado y de esta forma se puede garantizar la tutela judicial efectiva que reza en la Constitución de la República del Ecuador.

Para Ojeda (2018) la Policía Nacional del Ecuador, en el contexto de América Latina, se encuentra a la vanguardia al contar con una herramienta informática que permite la obtención de informes telefónicos en el contexto de investigaciones relacionadas con delitos cibernéticos. Sin embargo, es necesario y fundamental que se otorguen los equipos tanto físicos como digitales necesarias, así como las capacitaciones permanentes a los miembros de investigación a fin de poder realizar un trabajo efectivo.

CAPITULO II. DISEÑO METODOLÓGICO

1.1. Tipo de investigación y Enfoque de investigación

La investigación científica constituye un enfoque fundamental y amplio para llevar a cabo estudios con un sólido respaldo y validez científica en diversas disciplinas a nivel internacional. La elección del enfoque adecuado resulta esencial para determinar cuál es el más apropiado para cada estudio, y en el caso de las ciencias sociales, como el derecho, que abordan fenómenos intrínsecamente subjetivos y no cuantificables por naturaleza, la investigación jurídica se inclina generalmente hacia un enfoque cualitativo (Pons, 2017).

En la presente investigación, se aplicaron varios métodos para llevar a cabo una investigación cualitativa efectiva. Se utilizó un método teórico y analítico para analizar el dogma que rodea la figura de los ciberdelitos, recopilando, analizando y sintetizando información de diversas fuentes, como revistas, libros, artículos científicos y documentales, que abarcaban la doctrina relacionada con estos delitos en el contexto del principio de tutela judicial efectiva.

Este enfoque permite descubrir las relaciones esenciales y las cualidades fundamentales en el objeto de investigación que no serían detectables de otra manera. Se apoya en procesos de abstracción, análisis, síntesis, inducción y deducción, corrigiendo y enriqueciendo el conocimiento ordinario con los resultados de la ciencia (Hernández, 2015).

Además, se emplea un método analítico, que, según Santillana (2019), implica revisar las características de un objeto descomponiéndolo en sus partes constituyentes, observando periódicamente cada una para identificar su dinámica particular y las relaciones que dan origen a las características generales que se buscan comprender.

Asimismo, se utiliza el Método Deductivo, según Hernández (2017), que consiste en un proceso de análisis opuesto al inductivo. Se parte de principios generales aceptados como válidos por la ciencia, y mediante el razonamiento lógico y la síntesis, se pueden deducir suposiciones o explicar hechos particulares. Este método implica la extracción de consecuencias de algo generalmente aceptado, mediante la comparación y demostración en un proceso sintético-analítico del todo a la parte.

1.2. Tipo de recolección de la información

La modalidad de investigación seleccionada es documental, centrándose en fuentes primarias como las resoluciones judiciales. Esta técnica cualitativa implica recopilar y seleccionar información a través de la lectura de diversos documentos, como libros, revistas, grabaciones, filmaciones, periódicos, entre otros (Romero, 2021). En particular, la investigación documental se enfoca en indagar y hallar documentos como libros, revistas, periódicos, memorias, anuarios, registros, códices, constituciones, entre otros, para obtener información sobre el tema de estudio (Romero, 2021).

Dentro de la investigación documental, se destaca la investigación secundaria, que engloba la investigación bibliográfica y otras revisiones. Este enfoque metodológico es independiente de si se concibe como cuantitativo o cualitativo, y en este caso, busca determinar la existencia de resoluciones judiciales relacionadas con ciberdelitos y verificar si garantizan la tutela judicial efectiva (Pons, 2017).

La elección del tipo de investigación es fundamental, ya que existen diversas estrategias metodológicas. En este contexto, la presente investigación adopta la modalidad bibliográfica-documental, centrándose en el análisis sistemático de problemas relacionados con los ciberdelitos y la tutela judicial efectiva (Hernández, 2015).

El diseño de investigación, que constituye el plan general a seguir para obtener respuestas a los interrogantes planteados, se ajusta a la estrategia documental. Esta modalidad facilita la recolección de datos de la realidad de manera clara y no manipulada. Además, se basa en fuentes primarias y secundarias, donde las primarias incluyen testimonios de eventos presenciados y las secundarias son interpretaciones realizadas posteriormente por aquellos que no participaron directamente en los eventos (Ppons, 2021).

Fuentes Primarias

Las fuentes primarias son documentos que constituyen material directamente vinculado a una fuente original o evento en el momento en que ocurrió, siendo la materia prima para investigaciones o relatos. Estas fuentes contienen información no filtrada ni interpretada por terceros, siendo el producto de investigaciones o actividades creativas (Roomero, 2021).

En el contexto de esta investigación, los principios explícitos se han obtenido de fuentes primarias como libros, revistas científicas y de entretenimiento, periódicos, diarios, documentos oficiales de instituciones públicas, informes técnicos de instituciones públicas o privadas, patentes y normas técnicas (Hernández, 2015). Estas fuentes primarias proporcionan información original y nueva, resultado de un trabajo intelectual que respalda el análisis de los procesos de investigación en ciberdelitos, con el objetivo de garantizar la tutela judicial efectiva.

Fuentes secundarias

Las fuentes secundarias contienen información organizada, elaborada, producto de análisis, extracción o reorganización que refiere a documentos primarios originales, son fuentes secundarias: enciclopedias, antologías, directorios, libros o artículos que interpretan otros trabajos o investigaciones, contienen información primaria,

sintetizada y reorganizada. Están especialmente diseñadas para facilitar y maximizar el acceso a las fuentes primarias o a sus contenidos. Componen la colección de referencia de la biblioteca y facilitan el control y el acceso a las fuentes primarias.

1.3. Procesamiento y análisis de la información

Dentro de la presente investigación se llevará a cabo la técnica de la entrevista, la cual está dirigida hacia determinados fiscales según el número de denunciar recibidas por ciberdelitos en el año 2023. Bajo las mismas se estableció un cuestionario de esta manera, el proceso investigativo que se realizó pudo integrar las etapas específicas e interrelacionadas, que son esenciales en una entrevista cualitativa las cuales deben ser analizadas de manera reflexiva.

La entrevista es un instrumento de recolección de datos a partir de la interacción de dos partes: el entrevistador y el entrevistado. Si bien es un cuestionario, este mecanismo supone la intervención de una persona calificada o entrenada que deberá conducir la aplicación del instrumento. Esta figura es una especie de mediador que guía la recolección de información, organiza y controla la aplicación del cuestionario y registra las respuestas (Romero, 2021).

1.4. Población y muestra

Dentro de este apartado es esencial mencionar lo que Agramonte (2021) sostiene, la población y muestra es propio de una investigación científica, porque es el campo de donde se extrae la información que sirve como sustento de verificación de la investigación. En ese sentido, es esencial determinar que, al ser esta una investigación con enfoque cualitativo, la población recae en general en la sociedad de Ecuador víctima de la ciberdelincuencia, es por ello que, se ha elegido por parte de la investigadora, el muestreo no aleatorio, esto quiere decir que es la investigadora quien escoge a quienes y a cuantos profesionales entrevistar.

En ese caso, se ha procedido a escoger a tres abogados penalistas, tres especialistas en ciberseguridad/ ciberdelitos y a tres personas especialistas en seguridad bancaria (digital).

CAPÍTULO III: ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

En este capítulo se analiza la información otorgada por parte de los entrevistados respecto al tema de investigación, se procesa la misma con el método analítico sintético empleado por la investigadora.

Los resultados de la investigación se plasman a través de tablas que contienen las respuestas emitidas por parte de los profesionales entrevistados, ya que, gracias a las mismas se corrobora la hipótesis planteada. Es por ello que, las tabulaciones de las entrevistas se mencionan de manera literal, seguidas del análisis y la interpretación realizada por parte de la investigadora.

3.1. Presentación de resultados de los abogados especialistas en Derecho Penal.

Tabla 3 Resultados de abogados penalistas

Pregunta	Dr. Christian Gavilánez	Dr. Paulo Jordán	Dra. Andrea Altamirano
¿Podría definir a los ciberdelitos?	Si son infracciones, antijurídicas que afectan bienes tutelados por el derecho penal en los cuales han sido establecidos como una innovación de los delincuentes quienes se aprovechan de este tipo de espacios para beneficiarse de forma directa o indirecta. No en todas las legislaciones se los ha tipificado como ciberdelitos, sin embargo, se ha subsumido a la conducta en tipos penales previamente establecidos como son: Abuso de confianza, estafaba, aprovechamiento por medios electrónicos, extorsión, hostigamiento, acoso sexual, entre otros.	Los ciberdelitos son delitos especiales, que no tienen que ser confundidos con definiciones generales con los delitos informáticos, porque existen diferenciaciones a nivel teórico, estos delitos buscan proteger el bien jurídico de la seguridad de la información y los datos, que se encuentren en formatos electrónicos, así como de los sistemas informáticos. Es importante, tomar en cuenta que dicha protección debe abarcar, el acceso, el procesamiento y trasmisión de dicha información.	Podríamos llamar ciberdelitos a toda aquella infracción que haya sido ejecutada por un medio digital, utilizando medios informáticos o dispositivos de información telemática.
¿Considera Ud. que los ciberdelitos se producen por la negligencia del usuario? Si ¿por qué? No ¿por qué?	Tiene una doble respuesta, en parte no, porque el usuario es un poseedor de buena fe de un medio electrónico en el cual, bajo principio de confianza, confía que su actividad lícita o va a ser vulnerada, por otro lado, puede que tenga parte de responsabilidad por no, prever un posible ataque una seguridad básica que por falta de inversión deciden, no proteger de mejor manera, su patrimonio específicamente. El análisis de si, si o si no, debe ser en acuerdo al tipo de bien jurídico	Si, en la mayoría de los casos, esto se debe a la falta de educación por parte de un gran número de ciudadanos en materia de tecnologías de la información, es evidente que varios delitos son cometidos incluso a través de correo electrónico, como fishing, por medio del cual, a través de un engaño, que posiblemente sea muy fácil de detectar, personas entregan datos sensibles de su información financiera, social etc. Sin embargo, es evidente que cada día las mafias que rodean a estos delitos desarrollan técnicas más	Si existe desconocimiento del manejo informático de las herramientas que provee la institución, debida capacitación y no existe la para su manejo, y no existe el conocimiento acerca de las repercusiones del mal manejo informático.

	protegido que se afecta y al delito que se pretende consumar.	complejas que obligan a ciudadanos y autoridades, a educarse y trabajar en conjunto para combatir estos crímenes.	
Según Larrea (2020) los ciberdelitos pueden evitarse, ¿Concuerda con este criterio? Si ¿por qué? No ¿por qué?	Todo tipo de delito es evitable, sin embargo, las infracciones penales tienen una característica fundamental y es que son impredecibles, en este sentido yo puedo, precautelar o gratar de evitar mi bien jurídico protegido, sin embargo, no siempre voy a tener un resultado óptimo, puesto que como avanzan las medidas de seguridad también avanzan los medios delincuenciales para el cometimiento.	Sí, porque como en varios aspectos del ámbito penal, la prevención juega un rol importante y a más de esto, como se mencionó antes la educación en cuanto a las personas de tecnologías de la información es esencial, estos delitos pueden evitarse, en tanto a nivel social también exista una adecuada distribución de información, que permite al ciudadano ser más cauteloso al contratar bienes y servicios, tan simples como acceder a una banca virtual. Este tema se vuelve más complejo cuando hablamos de empresas, personas jurídicas, corporaciones, que manejan datos sensibles a nivel financiero, así como datos personales, teniendo que distinguir que varios de estos datos son manejados en empresas transnacionales. Viene a mi mente los casos de vulneración de los sistemas de empresas como Facebook, el banco pichincha, cnt, con la ley de protección de datos… se ha creado un marco normativo, que debería La aparición de la ley que es relativamente nueva es un avance importante en la protección de datos y de información como conocemos existe multas, que obligan desde las compañías hasta personas naturales a implementar sistemas y protocolos que garantice la protección de datos.	Pienso que sí, porque esto depende de la comunicación y capacitación da la ciudadanía, acerca de la protección de claves y de protección de la información sensible, así como también el alcance de la herramienta informática, ejemplo, el uso de la banca en línea, ahí vienen los fraudes, usurpaciones de identidad, jaqueo etc, la gente no sabe el manejo adecuado por falta de capacitación.

Según la estadística de fiscalía los delitos más frecuentes se dan, a través de las transferencias electrónicas, a su criterio, ¿cuál es el ciberdelitos más frecuente o que más ha escuchado?	Apropiación fraudulenta por medios electrónicos Art. 190 COIP Estafas, incluso extorciones. Hostigamiento, contravención en contra del honor y buen nombre. No es tan común, pero si ocurre, violaciones a la intimidad, extorsión sexual.	Dejando de lado aspectos teóricos delitos cometidos a través de sistemas informáticos o tecnologías de la información son contravenciones y delitos a través de redes sociales, además de delitos como apropiación fraudulenta de medios electrónicos, revelación ilegal de base de datos, tipificados en el COIP, interceptación ilegal de datos, o el ataque ilegal de sistemas informáticos.	Los robos en las bancas en línea, las transferencias con tarjetas de crédito, ya que en ellas se da muchos el jaqueo de claves y usurpación de identidad.
¿Cómo puede Ud. describir los grados de participación de las personas que cometen un ciberdelito?	Los grados de participación, varían de la forma y medio de cómo se comete el ilícito, esto es el *iter criminis*, para establecer el nivel de autoría, directa, mediata, coautoría, o complicidad conviene analizar los presupuestos facticos atinentes a cada caso, no se puede generalizar, puesto que el hecho ilícito, varía entre cada uno de sus acontecimientos y circunstancias, dentro del ciberdelito, comúnmente, se va a establecer una autoría directo, sin embargo, si es el medio para cometer otro ilícito, podría encontrarse una mediata o una coautoría.	Para describir los grados de participación dentro de estos tipos de delitos, dependerá de cada caso concreto, es decir de la casuística, en ese sentido al menos en ecuador, es importante tomar en cuenta las disposiciones del COIP de acuerdo con los grados de participación. Hablamos de autores y cómplices. Por ejemplo, si un individuo crea un sistema informático dirigido exclusivamente para el cometimiento de ciberdelitos, posiblemente estaríamos hablando de una autoría mediata, a través de ordenes realizados a través de medios fraudulentos, pero que ocurre si dicho medio o sistema, fue comercializado por esta persona, y posteriormente no tuvo participación alguna de la infracción, existía la responsabilidad, ¿posiblemente no?	Autor y cómplice, porque la gente que realiza los ciberdelitos son un grupo, pero siempre pueden tener un cómplice y ayuda, ejemplo, jaqueo Banco Pichincha, catalogaría como autor y cómplices al menos.
¿Podría explicar las modalidades o acciones para	Modalidades de conducta pueden ser de dos formas, la acción, la omisión que a su vez puede ser culposa y dolosa, si hablamos de la legislación ecuatoriana,	Yo considero que los ciberdelitos deben ser cometidos por acción y debe existir dolo, podría darse el caso de omisión, en cuanto de implementación	Debe ser dolosa, porque la persona que está jaqueando lo hace con engaño y la premeditación y actúa bajo engaño, el delincuente simula ser el banco, y la

cometer los ciberdelitos?	solamente solo se podría cometer ciberdelitos por acción y por omisión dolosa, la omisión culposa es excepcional para aquellos tipos penales que la establezcan como tal, que entre los ya indicados de manera previa, ninguno tiene el carácter culposo, sino dolosos.	de protocolos por parte de personas jurídicas, en cuanto al protección de datos y sistemas de protección.	gente entrega datos, prevalece el dolo, raro el caso, es que a la persona se le escapo el dato, debe ser una acción dolosa. Son delitos de acción, porque de omisión muy pocas, tal vez omisión del cuidado, pero los ciberdelitos son por dolo y engaño, premeditados es decir por acción.
Usted considera que si se regularía el proceso investigativo de ciberdelitos. ¿Se garantizaría el acceso a la tutela judicial efectiva? Si ¿por qué? No ¿por qué?	No, porque puedo llegar a tener una sentencia dependiendo del tipo penal y a su vez soi, porque no en todos los casos puedo determinar de forma efectiva la existencia material y responsabilidad del hecho, específicamente en casos de jurisdicción, competencia, y los bloqueos de delincuencia organizada	Considero que la solución parte de tener una norma sustantiva eficaz, y a la vez alineada con un sistema procesal, coherente con normativa internacional y de cooperación, con organismos internacionales, con conocimiento extenso y especifico en la materia, al ser fiscalía, la institución fundamental para la investigación de delitos, corresponde a esta, promover, a nivel orgánico y legislativo la adopción de normativa que permita el acceso a las personas a una justicia real.	Si pienso que la regulación de la investigación aportaría a tener más elemento para que se concrete un juicio, porque como sabemos la fiscalía, por ejemplo lo de las tarjetas lo manejan como mal uso de datos electrónicos, ellos dicen que solo pueden investigar el IP y eso no garantiza nada, o realizan desde teléfonos robados, no hay procesamientos científicos y tecnológicos que hagan el acompañamiento a este tipo de denuncias y quedan en el `papel, si incrementa la investigación, ayudamos a que se cumpla la tutela judicial de la que hablamos.
Considera Ud. ¿Qué el proceso investigativo en ciberdelitos es eficaz en Ecuador?	Hay una diferencia entre eficaz y eficiencia, es eficaz porque tenemos los medios, pero no es eficiente porque no cuento con el personal adecuado para el cumplimiento.	Considero que siempre se puede mejorar, es innegable, que en nuestro país, delitos informáticos que afectan al patrimonio de las personas en cuantías mínimas en su gran porcentaje quedan en la impunidad, por cuanto el ciudadano, debe someterse a un proceso de investigación penal, que involucra una inversión de tiempo, dinero, y muchas de las veces sin garantía de resultados, lo cual se	No, fiscalía debe tener mejores herramientas tecnológicas para poder investigar, y requiere del apoyo necesario de instituciones para poder realizar el seguimiento a dicho fraude.

		complica aún más, en este tipo de delitos en los cuales, la misma fiscalía, y la misma victima dependen de empresas con jurisdicciones internacionales.	
¿Qué mecanismos de investigación conoce para los ciberdelitos en el Ecuador?	Bueno en Ecuador los peritajes informáticos a través de los cuales se puede obtener la ubicación, datos de identificación de las personas que cometieron el delito.	Peritajes de índole informática, explotación de dispositivos, intervención de aparatos electrónicos o redes sociales.	1. La investigación de los IP aunque sabemos no es eficiente, pero en ciertos casos es útil. 2. La investigación de la guía de transacciones si hablamos del ámbito bancario. 3. Expertos en delitos informáticos, pero no sabría decir el alcance de su conocimiento, la tecnología está constantemente en avance.

Elaborado por: Carolina Castillo
A partir de: Instrumentos aplicados a los abogados especialistas en derecho penal

Análisis de los resultados de los abogados penalistas

Los profesionales entrevistados coinciden en que los ciberdelitos son aquellos que se cometen a través del internet, utilizando mecanismos virtuales para perjudicar el patrimonio o la integridad de las personas. Debido a la era en la que nos encontramos actualmente, los delitos informáticos o ciberdelitos van tomando más acogida y se van adentrando más en la sociedad, es por esta razón que, las autoridades deben estar alerta y establecer las normas necesarias para proteger los bienes jurídicos tutelados de las personas. En ese sentido, la normativa penal se ha reformado, pero es necesario que, en la práctica se instituya un camino procesal, es decir, la etapa de investigación no solo exista, sino que también sea efectiva, esto con el fin de garantizar la tutela judicial efectiva.

3.2. Resultados de expertos en ciberseguridad.

Tabla 4 Resultados de expertos ciberseguridad

Pregunta	Ing. Sebastián Herdoíza	Ing. Jorge Córdova	Ing. Teresa Freire
¿Podría definir que son los ciberdelitos?	Para mí un ciberdelito es un intento de encontrar vulnerabilidades en un sistema para comprometer su información o su funcionalidad, depende de si el ciberataque va a ser enfocado en una persona natural o a una empresa, las reglas son diferentes, fines y tipos de ataques diferentes.	Actividades delictivas que tienen que ver con la parte informática	Los ciberdelitos son actividades ilegales o criminales que se llevan a cabo utilizando computadoras, redes electrónicas o dispositivos conectados a internet Pueden incluir el acceso no autorizado a sistemas informáticos, el robo de datos personales o financieros, el fraude electrónico, el acoso cibernético
¿Considera Ud. que los ciberdelitos se producen por la negligencia del usuario? Si ¿por qué? No ¿por qué?	El mayor parte de ciberdelitos son causados por el descuido de los usuarios, por la falta de protección de sus credenciales y la falta de conocimiento de los ataques, no obstante, las plataformas que te brindan servicios digitales, son responsables de proteger tu información de cualquier ataque.	En mayor parte si, de hecho, es el eslabón más débil de cualquier institución, más que cualquier cosa, es por falta de conocimiento y educación en el área de ciberseguridad.	Ocurren debido a la negligencia del usuario en ciertos casos, ya que el descuido en el manejo de contraseñas, el uso de redes no seguras o la falta de actualización de software pueden exponer a los usuarios a riesgos cibernéticos. No todos los ciberdelitos se originan por negligencia del usuario, ya que también pueden estar vinculados a brechas de seguridad en sistemas, vulnerabilidades técnicas o ataques sofisticados que no dependen directamente de las acciones del usuario.
Según Larrea (2020) los ciberdelitos pueden evitarse, ¿Concuerda con este criterio? Si	Si, se pueden evitar, en dependencia si es un ataque cibernético, o un tipo de estafa cibernético, un ataque es cuando una persona intenta romper tus seguridades eso es hacking, por más que estés preparado, siempre uno	Nunca estamos 100 porciento libres del ciberdelito, por más seguridades que tengamos, siempre estamos expuestos, no estamos 100 porciento protegidos, no podría evitarse.	Es posible reducir el riesgo de ciberdelitos tomando medidas preventivas como la capacitación en seguridad cibernética, el uso de software antivirus, el mantenimiento regular de

¿por qué? No ¿por qué?	puede correr riesgos de ataques, por ejemplo banco de pichincha, cnt, tienen información valiosa, dinero, y buscan atacar para romper tus seguridades, pero en una persona natural, es más común el fishing, en donde te envían correos o mensajes fraudulentos en donde te piden tu información, es un tipo de ataque social. Ingeniería social, cuando alguien descifra tu contraseña por investigaciones que hacen de ti, en diferencia de un ataque de fuerza bruta, es cuando intentan probar muchas contraseñas hasta que una ingrese, esos los ataques más comunes para los usuarios y fishing. Si o estas siendo parte de un ataque es más difícil que lo puedas evitar, pero si se puede evitar, las probabilidades cambian de acuerdo con el caso.	Controlar si, pero evitar al 100 porciento no.	sistemas y la adopción de buenas prácticas de seguridad Pero no se pueden evitar completamente, estas medidas pueden reducir significativamente la probabilidad de ser víctima de un ciberdelito.
Según la estadística de fiscalía los delitos más frecuentes se dan, a través de las transferencias electrónicas, a su criterio, ¿cuál es el ciberdelito más frecuente o que más ha escuchado?	Para mí el más frecuente es el ransomeware enfocado en las empresas y compañías es el más común porque es un tipo de extorción digital, básicamente te envían un virus, y codifican toda la información, y para obtener la clave de acceso los delincuentes te piden dinero, grandes cantidades, les paso a cnt, ese es el ataque que más se ve en las empresas, es que las empresas más le temen, y más seguridad se da.	Para mí el más frecuente sería el ataque por fishing, suplantación de identidades por correo electrónico, porque da sus credenciales, y se dan las transferencias electrónicas ilícitas, pero el principal detonante es el fishing.	Los ciberdelitos más frecuentes según datos de Ecuador, el phishing (suplantación de identidad para obtener información confidencial), el ransomware (bloqueo o cifrado de archivos para exigir un rescate), el fraude financiero en línea, el robo de información personal y el acceso no autorizado a sistemas informáticos.
¿Cuál considera usted es el principal	Depende, pero prácticamente es buscar blancos fáciles, empresas sin	Ingeniería social, es el estudio de la víctima, investigar redes sociales,	La ingeniería social (engaño para obtener información confidencial), la

modus operandi de los ciberdelitos?	protecciones, personas descuidadas, ellos buscan los puntos débiles, existen.	donde trabaja, redes sociales, cargo, investigación de una ingeniería social.	explotación de vulnerabilidades de software, la suplantación de identidad.
¿Usted considera que dentro de la investigación de ciberdelitos se pueden realizar peritajes cibernéticos para identificar al responsable de un ciberdelito?	Si, se puede, dependiendo del crimen que se esté realizando, ejemplo wpp te permite exportar el chat completo, las plataformas te permiten transportar todo así hayas eliminado la conversación, ciertas plataformas, es parte de las políticas de las empresas tienen un respaldo por seguridad, por si existen crímenes mediante las plataformas. Hay procesos que hacen más eficiente llegar al delincuente un proceso que yo conozco es el Iplogger, se rastrea la IP de la persona o del atacante, con acceso a la IP te da la ubicación del delincuente.	Si es posible, requiere de un estudio especializado en informática forense, en donde se obtienen las evidencias, cadena de custodio, pruebas, investigaciones, y si se puede llegar al responsable.	Sí, los peritajes cibernéticos son fundamentales en la investigación de ciberdelitos para identificar al responsable. Implican el análisis forense de dispositivos electrónicos, redes y sistemas informáticos para recopilar pruebas digitales.
Sabe Ud. Si en Ecuador ¿Existen peritos especialistas en este tipo de pruebas	Si hay, son los peritos forenses, Ing. en sistemas forenses, ellos se encargan de a criminalística informática, uno de los principios que ellos ocupan es que la información debe ser de primera mano, debe ser del dispositivo que grabo, debe ser fuente original.	Deben existir, pero no conozco ninguno, pero tienen que haber, porque existen los formatos para los informes.	Sí, en Ecuador existen profesionales especializados en peritajes cibernéticos y forenses digitales que colaboran con las autoridades en la investigación de ciberdelitos.
¿Conoce usted si en el Ecuador existen formación certificada para profesionales en ciberseguridad?	Existe y en la PUCESA. Certificados, maestrías y demás.	Una maestría se considera una formación certificada entonces sí, yo estoy terminando la maestría.	Sí, en Ecuador existen instituciones educativas y entidades que ofrecen programas de formación certificados en ciberseguridad, incluyendo cursos, diplomados y certificaciones reconocidas internacionalmente.
¿Qué mecanismos o alternativas se pueden emplear	Para las plataformas personales, 1 no ingresar a sitios web no certificados, 2do, mantener contraseñas robustas y	Existen muchos métodos, lo principal que hay que tener en cuenta es una seguridad por capas, contraseña	Uso de contraseñas fuertes y únicas, Autenticación de dos factores,

para evitar intrusos cibernéticos en nuestras plataformas personales o empresariales?	no repetidas, tercero, necesitas un antivirus. Para empresas es mejor utilizar firewals, redes privadas virtuales, vpns con la finalidad de proteger de manera genérica sus datos, considerar los protocolos apropiados para proteger sus datos.	segura, doble factor de autenticación, cumplir con los requisitos mínimos de seguridad, no tener apuntadas las contraseñas en el celular, multiniveles, mientras más capas de seguridad se pone, mayor de seguridad, pero no el 100 por ciento fiable que se quede libres.	La actualización regular del software y sistemas, la implementación de firewalls y software antivirus, la Capacitación en seguridad cibernética para empleados, y la realización de copias de seguridad periódicas de la información importante.

Elaborado por: Carolina Castillo
A partir de: Instrumentos aplicados a expertos en ciberseguridad

Análisis de los resultados de los expertos en ciberseguridad

Los expertos en ciberseguridad por su parte, manifestaron que, los ciberdelitos son más comunes de lo que se piensa actualmente, que ya tienen tiempo en la sociedad, pero con el desarrollo tecnológica y el acceso al mismo se han profundizado. Es necesario que, existan más personas especializadas en ciberseguridad, pero dentro de la función judicial, porque los institutos o preparación que se brinda es dentro del ámbito privado, cuando las investigaciones previas se llevan a cabo por medio de peritajes que hacen personas acreditadas por el órgano competente, en este sentido corresponde a las autoridades acreditar más expertos en ciberseguridad para que logren desarrollar una investigación efectiva.

3.3. Análisis general de resultados

De acuerdo con lo expuesto por los profesionales entrevistados, los delitos cibernéticos se caracterizan como transgresiones específicas y no se pueden confundir con conceptos más generales como los delitos informáticos. Estos delitos tienen como objetivo preservar el bien jurídico relacionado con la seguridad de la información y los datos almacenados en formatos electrónicos, así como garantizar la protección de los sistemas informáticos. Es esencial resaltar que esta salvaguardia incluye aspectos como el acceso, el procesamiento y la transmisión de dicha información.

El aumento del crimen cibernético refleja una tendencia creciente en la delincuencia transnacional y se destaca como uno de los tipos delictivos que experimenta un rápido crecimiento. A medida que Internet se ha vuelto prácticamente indispensable en nuestras vidas, facilitando la difusión de información y la comunicación a nivel global, los delincuentes han sabido capitalizar esta realidad. Con aproximadamente dos mil millones de usuarios en todo el mundo, el ciberespacio emerge como un entorno propicio para los criminales, quienes pueden mantener el anonimato y acceder a diversos tipos de información personal que consciente o inconscientemente almacenamos en línea.

Los delitos cibernéticos requieren una acción deliberada y la presencia de intención criminal, aunque también puede surgir una situación de omisión, como en el caso de la falta de implementación de protocolos por parte de entidades legales en lo que respecta a la protección de datos y sistemas de seguridad. La Fiscalía, como entidad fundamental para la investigación de delitos, tiene la responsabilidad de promover, tanto a nivel organizativo como legislativo, la adopción de normativas que faciliten a las personas el acceso a una justicia genuina y efectiva.

En Ecuador, la mayoría de los delitos informáticos que afectan el patrimonio de las personas, especialmente aquellos de menor cuantía, a menudo quedan

impunes. Esto se debe a que los ciudadanos se ven obligados a someterse a procesos de investigación penal que demandan tiempo y recursos financieros, sin la certeza de obtener resultados positivos. La complejidad aumenta aún más en este tipo de delitos, ya que tanto la fiscalía como la víctima dependen de empresas con jurisdicciones internacionales. Es por ello que, si se puede mejorar la investigación penal, sobre todo en el tema de peritajes e informes especializados para esta clase de delitos.

Respecto de la información recabada de los expertos en ciberseguridad se tiene que los peritajes en informática tienen que ver con aquellas diligencias e intervenciones en la nube o dirigidas a los dispositivos de las partes involucradas en un delito de carácter informático, para que se pueda determinar la ubicación o identificación del infractor. Y en Ecuador si existen peritos especializados en esta clase de evaluaciones y exámenes incluso existen lugares en donde se pueden formar en esta rama y así *a posteriori* puedan formar parte de los ingenieros forenses.

CONCLUSIONES

- Se analizó la figura de los procesos investigativos de *ciberdelitos* concluyendo que, en Ecuador al momento del cometimiento de un *ciberdelito* se inicia una investigación previa, la misma que, bajo la objetividad de Fiscalía General del Estado recaba elementos de cargo o de descargo. En ese sentido, los delitos de carácter cibernético, ameritan la evacuación de algunos peritajes destinados a conocer la identidad y ubicación del autor del delito, dichos peritajes descritos en la página 62 de la investigación, como las explotaciones de audio, video y afines, identificación de ID e IP, etc., para que de esta forma se pueda seguir con el proceso penal y la víctima pueda ser reparada en su bien agraviado, garantizando de esta forma la tutela judicial efectiva.

- Se fundamentó doctrinaria y jurídicamente a los *ciberdelitos*, en tanto que se estudiaron las teorías del Comportamiento Planificado de Ajzen y la teoría del Flujo de Beveren, por lo que se concluye que, son aquellas conductas típicas, antijurídicas y culpables que se cometen a través de la red, o también conocida como internet, que perjudica un bien jurídico tutelado de otra persona. Esta clase de delitos se maneja de forma virtual y no es necesario que la víctima y el victimario interactúe de forma presencial, perjudicando el patrimonio u otros bienes jurídicos tutelados de forma conexa.

- Se diagnosticó que, la tutela judicial efectiva, en teoría se garantiza dentro de los procesos investigativos de ciberdelitos, toda vez que, permiten acceder a un proceso o iniciar con una denuncia o por medio de las diferentes *noticia criminis* que permite la legislación ecuatoriana; pero, ya en el transcurso de la investigación, las diligencias que se manejan en el sistema ecuatoriano no permiten una efectiva respuesta, por lo que es muy complicado llegar a la verdad de los hechos, individualizar al o los sospechosos; por ende, llevar el caso al conocimiento de un juez penal. Es por ello que, la tutela judicial no es efectiva.

- Se identificó que, en Ecuador, los ciberdelitos han sido incorporados a la norma penal, Código Orgánico Integral Penal, de tal forma que se puedan salvaguardar a las personas en torno al manejo y uso de redes virtuales, plataformas y transacciones que se realicen a través de la internet. Por lo que, se garantiza a la ciudadanía activar la administración de justicia para restituir el bien agraviado. Con este presupuesto se consolida el principio de tutela judicial efectiva, principio que básicamente se trata de garantizar a las personas el llevar un proceso judicial que cumpla con todas las garantías básicas del debido proceso y concluya con una resolución apegada a la verdad y garantice los derechos tanto de la víctima como del victimario.

RECOMENDACIONES

- Se recomienda a la administración central para que, elabore las políticas públicas necesarias y que se encaminen a brindar la seguridad a la ciudadanía que se requiere para evitar que sus plataformas se queden a buen recaudo. Concientizando a la población en general para manejar sus plataformas de la manera adecuada y sin confiar en terceras personas, se lograría mitigar en algo la ciberdelincuencia.

- Se recomienda también a toda la ciudadanía tener responsabilidad en su seguridad digital, crear contraseñas seguras en sus redes sociales, con doble autenticación, y hay que seguir las políticas de privacidad en cada una de las plataformas a las que ingresen, de preferencia no ingresar a redes de internet públicas, y si lo hacen, no ingresar claves, ni realizar transferencias bancarias, teniendo en cuenta que toda la información personal del dispositivo que ingresa a la red se queda guardado en la misma.

- Se recomienda a la Fiscalía General del Estado para que capacite continuamente a los peritos forenses en el ámbito informático, para que se encuentren preparados y listos para que elaboren peritajes de calidad y generen eficacia al proceso investigativo de cualquiera de los ciberdelitos contenidos en el Código Orgánico Integral Penal. Estas capacitaciones deberán estar enfocadas en los peritajes apropiados para poder determinar la individualidad de los sospechosos y la ubicación de estos, con eso se hace efectiva la investigación, caso contrario, se incurre el gasto al Estado, en aperturar una investigación que no va a llegar a ningún lado.

BIBLIOGRAFIA

Aguirre, V. (2020). El Derecho a la tutela judicial efectiva: una aproximación a su aplicación por los tribunales ecuatorianos. Foro *Revista de derecho*, N° 14.

Alarcón, D., & Barrera, J. (2017). Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede seccional Sogamoso. Universidad Norbert Wiener: http://repositorio.uwiener.edu.pe/bitstream/handle/123456789/1630/MAESTRO%20%20%20Barrera%20Bar%c3%b3n%2c%20Javier%20Antonio.pdf?sequence=1&isAllow ed=y

Araujo, M. (2017). Acceso a la justicia y tutela judicial efectiva. Propuesta para fortalecer la justicia administrativa. Visión de derecho comparado. *Estudios Sociojurídicos* 13, n. 1. https://revistas.urosario.edu.co/index.php/sociojuridicos/article/view/1513.

Asamblea Nacional del Ecuador. (2008). Constitución de la República del Ecuador. Quito: Registro Oficial No. 449.

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Quito: Registro Oficial No. 180.

Asamblea Nacional del Ecuador. Código Orgánico de la Función Judicial. R.O. 544

Bermúdez, Á. (2019)Brexit - cierre del gobierno: por qué Reino Unido y Estados Unidos acabaron sumidos en crisis políticas tan graves y quiénes son los grandes beneficiados. https://www.bbc.com/mundo/noticias-internacional46901065.

Campbell, K. (2019). Lessons from the cyberattack on India's largest nuclear power plant", Bulletin of the Atomic Scientists. https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largestnucl/?utm_source=Newsletter&utm_medium=Email&utm_campaign=Newsletter11142019&utm_content=NuclearRisk_Cyberattack_11142019 .

Chas, G. (2021). El gran desafío de la Justicia es combatir al cibercrimen. https://www.nortecorrientes.com/172084-segunguillermo-chas--el-gran-desafio-de-la-justicia-es-combatir-al-cibercrimen

Chicharro, A. (2019). La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas. Revista de Internet, Derecho y Política. https://dialnet.unirioja.es/servlet/articulo?codigo=3101795

CJ Consejo de la Judicatura (2018). Base de datos Sistema Automático de Trámite Judicial Ecuatoriano (SATJE). Base Excel de datos estadísticos de delitos informáticos 2014-2018.

Corte Constitucional del Ecuador. Sentencia N.° 015-16-SEP-CC, caso N.° 1112-15-EP, 13 de enero del 2016.

Corte Constitucional del Ecuador. Sentencia N.° 030-10-SCN-CC, caso N.° 0056-10-CN, 10 de marzo de 2014.

Corte Constitucional del Ecuador. Sentencia N.° 1234-14-EP/20, caso N.° 1234-14-EP, 11 de marzo del 2020.

Corte Constitucional del Ecuador. Sentencia N.° 1943-12-EP/19, caso No. 1943-12-EP, 25 de septiembre del 2019.

Corte Constitucional del Ecuador. Sentencia" N.° 364-16-SEP-CC, caso N.° 1470-14-EP, 15 de noviembre del 2016.

Cybersecurity Ventures. (2019). Official Annual Cybercrime Report. *Herjavec Group.* https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Dammert, L., & Lunecke, A. (2018). La prevención del Delito en Chile. Una visión desde la comunidad. Santiago de Chile: Cesc.

De Sousa, Boaventura (2021). Derecho y Emancipación. Quito: Centro de Estudios y Difusión del Derecho Constitucional. Ecuador.

Días, L. (2021). La Garantía Procesal del Debido Proceso. Lima: Cultural Cuzco S.A.

Ecuador, Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). Acuerdo Ministerial No. 012-2019. Quito: Registro Oficial No.18 de 15 de agosto de 2019.

EcuRed. (2022). Impacto de las tecnologías en los países del Tercer Mundo. https://www.ecured.cu/Impacto_de_las_tecnolog%C3%ADas_en_los_pa%C3%ADses_del_Tercer_Mundo#Paradojas_en_la_era_de_la_informaci.C3.B3n

Equipo de comunicaciones y Escuela de Seguridad Digital. (11 de 10 de 2021). ¿Qué es una suplantación de identidad digital y cómo puede afectarte? Obtenido de Uso estratégico de 79 internet para el desarrollo: https://colnodo.apc.org/es/experiencias/que-es-unasuplantacion-de-identidad-digital-y-como-puede-afectarte

Erazo, E. (2019). Teoría de la motivación de las resoluciones judiciales y jurisprudencia de casación y electoral. Quito: V&M Gráficas. Lima: ARA Editores, 2003.

España, Congreso Nacional. (1995). Código Penal. Madrid: Boletín Oficial del Estado (BOE), N° 281, del 24 de noviembre de 1995.

Garcia, E. (2017). Dominant and Subjugated Explanatory Narratives. En Cybercrime, Organized Cryme and Societal Responses. International Approaches, de Emilio C. Viano. Cham: Springer.

García, J. (2022). Derecho Procesal Constitucional, *Editorial TEMIS.* 25, http://garciabelaunde.com/Biblioteca/DProcesalConstitucional.pdf.

Hernández Sampieri, R, Fernández, C & Baptista, P. (2010). Metodología de la Investigación. (Quinta Edición). México D.F, México: McGraw-Hill.

Herrero, C. (2017). Criminología parte general y especial. Madrid: Dykinson

Larios, J., & Sánchez, R. (2018). Ciberdelito. https://4884/Tesis. pdf?sequence=2&isAllowed=y

Lemaitre, R. (2020). La impunidad de los delitos informáticos en la ciber sociedad costarricence en el ámbito del derecho penal. Universidad de Costa Rica: https://iij.ucr.ac.cr/wp-content/uploads/bsk-pdfmanager/2017/06/La-Impunidad-de-los-Delitos-Inform%C3%A1ticos-en-la-Cibersociedad-Costarricense.pdf

Meléndez, J. (25 de Julio de 2018). Delito informáticos o ciberdelitos. Derecho Ecuador: https://derechoecuador.com/delitos-informaticos-ociberdelitos/

Ochoa, A. (2021). Desafíos globales del cibercrimen. Caso Ecuador. Período 2014-2019. Recuperado el 8 de enero de 2022, de Universidad Andina Simón Bolívar: https://repositorio.uasb.edu.ec/bitstream/10644/7919/1/T3432-MRI-Ochoa-Desafios.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito. (2019). Ciberespionaje. Serie de Módulos Universitarios: Delitos Cibernéticos: https://www.unodc.org/e4j/es/cybercrime/module-14/keyissues/cyberespionage.html

Oficina de las Naciones Unidas contra la droga y el Delito. (2019). El uso de internet con fines terroristas. https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_ Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Ojeda, J., Arias, M., Rincón, F., & Daza, L. (2018). Delitos informáticos y entorno jurídico vigente en Colombia. Bogotá: Cuadernos de Contabilidad.

Ortiz, K. (2019). Cyber-Grooming Young Women for Terrorist Activity.

Ponluisa, A. (2021) El acceso a la justicia a la luz del Estado social de Derecho en Colombia. *Revista Científica Gen*. N.° 16. http://webcache.googleusercontent.com/search?q=cache:http://www.scielo.o rg.co/pdf/recig/v13n16/v13n16a05.pdf

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO - Revista Latinoamericana de Estudios de Seguridad, https://revistas.flacsoandes.edu.ec/urvio/article/view/2563/2108.

Ramos. J. (2019). Cybercrimen, digital forensics and jurisdiction. New York: Springer International.

Rojas, W. (2019). Criminal Proceedings in Cyberspace: The Challenge of Digital Era". En Cybercrimen, organized crimen and Societal Responses, compilado por Emilio C. Viano. Cham: Springer International Publishing Switzerland.

Roma, L. (2022). Los juzgados constitucionales para una protección eficaz de los derechos en el Distrito Judicial de Áncash", https://www.researchgate.net/publication/328970124_Los_juzgados_constitucionales_para_una_proteccion_eficaz_de_los_derechos_constitucionales_en_el_Distrito_Judicial_de_Ancash

Romero, K. (2021). Metodología de la investigación jurídica. Quito: Corporación Nacional de Estudios y Publicaciones.

Salas, D. (2019). Regulación de Internet y derechos digitales en Ecuador. Quito: Universidad San Francisco de Quito.

Vergara, L. (2018). El concepto de criminalidad organizada transnacional: problemas y propuestas. *Revista Nuevo Foro Penal* 12 (86).

ANEXOS

Anexo N. 1 Entrevistas para los especialistas en derecho penal

N	Pregunta
1	¿Podría definir a los ciberdelitos?
2	¿Considera Ud. que los ciberdelitos se producen por la negligencia del usuario?
3	Según Larrea (2020) los ciberdelitos pueden evitarse, ¿Concuerda con este criterio?
4	Según la estadística de fiscalía los delitos más frecuentes se dan, a través de las transferencias electrónicas ¿a su criterio, ¿cuál es el ciberdelito más frecuente?
5	¿Cómo puede Ud. Describir los grados de participación de las personas al cometer ciberdelitos?
6	¿Podría explicar las modalidades o acciones para cometer los ciberdelitos?
7	Usted considera que si se regularía el proceso investigativo de ciberdelitos. ¿Se garantizaría el acceso a la tutela judicial efectiva?
8	Considera Ud. ¿Qué el proceso investigativo en ciberdelitos es eficaz en Ecuador?
9	¿Qué mecanismos de investigación conoce para los ciberdelitos en el Ecuador?

Elaborado por: La investigadora.

Anexo N. 2 Entrevistas para los especialistas en ciberseguridad

N	Pregunta
1	¿Podría definir que son los ciberdelitos?
2	¿Considera Ud. que los ciberdelitos se producen por la negligencia del usuario?
3	Según Larrea (2020) los ciberdelitos pueden evitarse, ¿Concuerda con este criterio?
4	Según la estadística de fiscalía los delitos más frecuentes se dan, a través de las transferencias electrónicas ¿a su criterio, ¿cuál es el ciberdelito más frecuente?
5	¿Cuál considera usted es el principal modus operandi de los ciberdelitos?
6	¿Usted considera que dentro de la investigación de ciberdelitos se pueden realizar peritajes cibernéticos para identificar al responsable de un ciberdelito?
7	¿Sabe usted si en Ecuador existen peritos especialistas en este tipo de pruebas?
8	¿Conoce usted si en Ecuador existe formación certificada para profesionales en ciberseguridad?
9	¿Qué mecanismos o alternativas se pueden emplear para evitar intrusos cibernéticos en nuestras plataformas personales o empresariales?

Elaborado por: La investigadora.

Anexo N. 3. Profesionales a quienes se dirige la entrevista

Nombre	Cargo
Ab. Ms. Christian Gavilánez	Abogado especialista en Derecho penal
Ab. Ms. Paulo Jordán	Abogado especialista en Derecho penal
Ab. Ms. Andrea Altamirano	Abogada especialista en Derecho penal
Ing. Sebastián Herdoíza	Experto en ciberseguridad
Ing. Jorge Córdova	Experto en ciberseguridad
Ing. Teresa Freire	Experta en ciberseguridad

Elaborado por: La investigadora.